



Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 12.2(54)SG to 12.2(37)SG

Current Release

12.2(54)SG1—February 7, 2011

Previous Releases

12.2(54)SG, 12.2(53)SG9, 12.2(53)SG8, 12.2(53)SG7, 12.2(53)SG6, 12.2(53)SG5, 12.2(53)SG4, 12.2(53)SG3, 12.2(53)SG2, 12.2(53)SG1, 12.2(53)SG, 12.2(52)X0, 12.2(52)SG, 12.2(50)SG8, 12.2(50)SG7, 12.2(50)SG6, 12.2(50)SG5, 12.2(50)SG4, 12.2(50)SG3, 12.2(50)SG2, 12.2(50)SG1, 12.2(50)SG, 12.2(46)SG, 12.2(44)SG1, 12.2(44)SG, 12.2(40)SG

These release notes describe the features, modifications, and caveats for the Cisco IOS software on the Catalyst 4500 series switch. The most current software release is Cisco IOS Release 12.2(54)SG.

Support for Cisco IOS Software Release 12.2(54)SG, the default image, follows the standard Cisco Systems® support policy, available at

http://www.cisco.com/en/US/products/products_end-of-life_policy.html



Note

Although their *Release Notes* are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M/4948E) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*.

For more information on the Catalyst 4500 series switches, visit the following URL:

<http://www.cisco.com/go/cat4500/docs>

Contents

This publication consists of these sections:

- [Cisco IOS Software Packaging for the Cisco Catalyst 4500 Series](#), page 2
- [Orderable Product Numbers](#):, page 8
- [Catalyst 4500 Series Switch Cisco IOS Release Strategy](#), page 11



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 1999-2011 Cisco Systems, Inc. All rights reserved.

- [System Requirements, page 12](#)
- [New and Changed Information, page 30](#)
- [Upgrading the System Software, page 44](#)
- [Limitations and Restrictions, page 56](#)
- [Caveats, page 69](#)
- [Troubleshooting, page 426](#)
- [Related Documentation, page 428](#)
- [Notices, page 429](#)
- [Obtaining Documentation and Submitting a Service Request, page 432](#)

Cisco IOS Software Packaging for the Cisco Catalyst 4500 Series

A new Cisco IOS Software package for Cisco Catalyst 4500 Series Switches was introduced in Cisco IOS Software Release 12.2(25)SG. It is a new foundation for features and functionality and provides consistency across all Cisco Catalyst switches. The new Cisco IOS Software release train is designated as 12.2SG.

Prior Cisco Catalyst 4500 Series IOS Software images for the Cisco Catalyst 4500 Series Switches, formerly known as Basic Layer 3 and Enhanced Layer 3, now map to IP Base and Enterprise Services, respectively. All currently shipping Cisco Catalyst 4500 software features based on Cisco IOS Software are supported in the IP Base image of Release 12.2(54)SG, with a few exceptions.

The IP Base image does not support enhanced routing features such as NSF/SSO, BGP, EIGRP, EIGRPv6, OSPF, OSPFv3, IS-IS, Internetwork Packet Exchange (IPX), AppleTalk, VRF-lite, and Policy-Based Routing (PBR). The IP Base image supports EIGRP-Stub for limited routing on Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, V-10GE, and 6-E.

The Enterprise Services image supports all Cisco Catalyst 4500 Series software features based on Cisco IOS Software, including enhanced routing. Customers planning to enable BGP for Supervisor Engine IV, V, or V-10GE will no longer need to purchase a separate BGP license (FR-IRC4) because BGP is included in the Enterprise Services package. Beginning with 12.2(53)SG2, we support the Enterprise Services image on Supervisor Engine 6L-E.

Cisco IOS Release 12.2(46)SG1 introduced a new LAN Base software and an IP upgrade image. These complement the existing IP Base and Enterprise Services images. The LAN base image is supported on the Supervisor Engine II-Plus-10GE and Supervisor Engine 6L-E starting with Cisco IOS Release 12.2(52)XO. LAN Base image is primarily focused on customer access and Layer 2 requirements and therefore many of the IP Base features are not required. The IP upgrade image is available if at a later date you require some of those features.

[Table 1](#) contrasts feature support on the LAN Base vs IP Base images.

For information on MiBs support, pls refer to this URL:

<http://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html>

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
10G Uplink Use	12.2(46)SG1	Yes	Yes
802.1p prioritization	12.2(46)SG1	Yes	Yes
802.1p/802.1q	12.2(46)SG1	Yes	Yes
802.1w/802.1s	12.2(46)SG1	Yes	Yes
802.1X (w/ Guest VLAN and VLAN Assignment)	12.2(50)SG	Yes	Yes
802.1X and MAB with ACL assignment	12.2(50)SG	Yes	Yes
802.1X (Auth-Fail VLAN, Critical Auth, Accounting)	12.2(50)SG	Yes	Yes
802.1X Wake on LAN	12.2(50)SG	Yes	Yes
802.1X Web-Auth	12.2(50)SG	Yes	Yes
802.1X with Multiple authenticated, multi-host	12.2(50)SG	Yes	Yes
802.1X w/ MDA	12.2(50)SG	Yes	Yes
802.1X w/ Open Access	12.2(50)SG	Yes	Yes
802.3ad LACP	12.2(46)SG1	Yes	Yes
802.3x – Flow Control	12.2(46)SG1	Yes	Yes
ACL Logging	12.2(46)SG1	Yes	Yes
All Mibs	12.2(52)SG	Yes	Yes
Auto QoS	12.2(53)SG	Yes	Yes
Auto SmartPort	12.2(54)SG	Yes	Yes
Auto-MDIX	12.2(46)SG1	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	No support	Yes	Yes
BOOTP	12.2(46)SG1	Yes	Yes
Bootup GOLD	No support	Yes	Yes
Broadcast Suppression	12.2(46)SG1	Yes	Yes
CDP/CDPv2	12.2(46)SG1	Yes	Yes
Community PVLAN support	No support	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
Config File	12.2(46)SG1	Yes	Yes
Console Access	12.2(46)SG1	Yes	Yes
Control Plane Policing	12.2(46)SG1	Yes	Yes
Copy Command	12.2(46)SG1	Yes	Yes
CoS to DSCP Map	Yes	Yes	Yes
Debug Commands	12.2(46)SG1	Yes	Yes
Device Management	12.2(46)SG1	Yes	Yes
DHCP Server	12.2(46)SG1	Yes	Yes
DHCP Snooping	12.2(46)SG1	Yes	Yes
Diagnostics Tools	12.2(46)SG1	Yes	Yes
Downloading Software	12.2(46)SG1	Yes	Yes
DSCP to CoS Map	12.2(46)SG1	Yes	Yes
DSCP to egress queue mapping	12.2(46)SG1	Yes	Yes
Dynamic ARP inspection	12.2(46)SG1	Yes	Yes
EEM and EOT integration	No support	Yes	Yes
EIGRP Stub	No support	Yes	Yes
EnergyWise 1.0	12.2(53)SG	Yes	Yes
EPoE	12.2(53)SG	Yes	Yes
Ethernet Management Port (Fa1 interface)	12.2(46)SG	Yes	Yes
Event Log	12.2(46)SG1	Yes	Yes
Factory Default Settings	12.2(46)SG1	Yes	Yes
File Management	12.2(46)SG1	Yes	Yes
Flex Link	12.2(53)SG	Yes	Yes
GLBP	No support	Yes	Yes
HSRP v1/VRRP	No support	Yes	Yes
HSRP v2 IPV4	No support	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
HSRP v2 IPV6	No support	No	Yes
ID 4.0 Voice Vlan assignment	12.2(46)SG1	Yes	Yes
ID4.1 Filter ID and per use ACL	12.2(46)SG1	Yes	Yes
IGMP	12.2(46)SG1	Yes	Yes
IGMP Snooping	12.2(46)SG1	Yes	Yes
Ingress Policing	12.2(46)SG1	Yes	Yes
Interface Access (Telnet, Console/Serial, Web)	12.2(46)SG1	Yes	Yes
IP Source Guard	12.2(46)SG1	Yes	Yes
IP Multicast	No support	Yes	Yes
IPv6 HSRP	No support	No	Yes
IPv6 MLD snooping V1 and V2	Future	Yes	Yes
IPv6 Reformation	NA	Yes	Yes
IPv6 Router Advertisement (RA) Guard	12.2(54)SG	Yes	Yes
ISL Trunk	12.2(46)SG1	Yes	Yes
ISSU	No support	Yes	Yes
Jumbo Frames	12.2(46)SG1	Yes	Yes
Layer 2 Debug	12.2(46)SG1	Yes	Yes
Layer 2 PT and QinQ	No support	Yes	Yes
Layer 2 Traceroute	12.2(46)SG1	Yes	Yes
Link State Tracking	12.2(54)SG	Yes	Yes
LLDP/LLDP-MED	12.2(52)SG	Yes	Yes
LLDP enhancements (PoE+Layer 2 COS)	12.2(54)SG	No	Yes
Local Web Auth	12.2(52)SG	Yes	Yes
MAB (MAC Authentication Bypass)	12.2(50)SG	Yes	Yes
MAC Address Filtering	12.2(50)SG	Yes	Yes
MAC Based Access List	12.2(50)SG	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
Management IPv6 port	12.2(52)SG	Yes	Yes
MLD Snooping	12.2(53)SG	Yes	Yes
Multicast Filtering	12.2(46)SG1	Yes	Yes
Multihop SXP (CTS)	No support	12.2(52)SG	Yes
Network Edge Access Topology (NEAT)	No support	Yes	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes	Yes
No. of VLAN Support	2048	4096	Yes
OSPF for Routed Access	No support	Yes	Yes
PAgP	12.2(46)SG1	Yes	Yes
Passwords Password clear protection	12.2(46)SG1	Yes	Yes
PIM SM/DM	No support	Yes	Yes
PoE (up to 15.4W only)	12.2(46)SG1	Yes	Yes
PoE+ Ready	Yes	Yes	Yes
Port Monitoring (interface Stats)	12.2(46)SG1	Yes	Yes
Port Security	12.2(46)SG1	Yes; only 1024 MACs	Yes
Post Status	12.2(46)SG1	Yes	Yes
PVST+	12.2(53)SG	Yes	Yes
Q-in-Q	No support	Yes	Yes
RACL (DSCP based)	12.2(46)SG1	Yes	Yes
RADIUS/TACACS+ (AAA)	12.2(46)SG1	Yes	Yes
RMON	12.2(46)SG1	Yes	Yes
Routing, Static	12.2(46)SG1	Yes	Yes
RIP	No	Yes	Yes
RPR	12.2(46)SG1	Yes	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base	Enterprise Services
RPVST+	12.2(53)SG	Yes	Yes
RSPAN	12.2(46)SG1	Yes	Yes
Service Advertisement Framework (SAF)	No support	No	Yes
Smart Call Home	No support	Yes	Yes
SmartPorts (Role based MACRO)	12/2(53)SG	Yes	Yes
SNMP (including SNMv3)	12.2(46)SG1	Yes	Yes
Source port Filtering (Private VLAN)	12.2(46)SG1	Yes	Yes
SPAN (# of sessions) – Port Mirroring	12.2(46)SG1 (2 sessions)	Yes (8 bidirectional sessions)	Yes
SSHv2/Secure Copy, FTP, SSL, Syslog, Sys Information	12.2(46)SG1	Yes	Yes
Storm Control	12.2(46)SG1	Yes	Yes
TDR	No support	Yes	Yes
Time Protocols (SNTP, TimeP)	12.2(46)SG1	Yes	Yes
Time Protocols (SNTP, TimeP) master	12.2(52)SG	Yes	Yes
Time-based ACL	12.2(46)SG1	Yes	Yes
Traffic Mirroring (SPAN)	12.2(46)SG1	Yes	Yes
Trusted Boundary (LLDP & CDP Based)	12.2(46)SG1	Yes	Yes
UDLD	12.2(46)SG1	Yes	Yes
VACL and PACL	12.2(46)SG1	Yes	Yes
VLAN Mapping (VLAN Translation)	12.2(54)SG	Yes	Yes
Voice VLAN	12.2(46)SG1	Yes	Yes
VRRP	No support	Yes	Yes
VTP	12.2(46)SG1	Yes	Yes
WCCP	No support	Yes	Yes
XML-PI	12.2(54)SG	Yes	Yes

Orderable Product Numbers:

- S49LB-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (LAN Base image)
- S49LBK9-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (LAN Base image with Triple Data Encryption)
- S49IPB-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (IP Base image)
- S49IPBK9-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (IP Base image with Triple Data Encryption)
- S49ES-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (Enterprise Services image with BGP support)
- S49ESK9-12254SG(=)—Cisco IOS Software for Cisco Catalyst 4500 Series Switch (Enterprise Services image with 3DES and BGP support)
- S45ES-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with Border Gateway Protocol [BGP] support, without Crypto)
- S45IPBK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard [3DES])
- S45IPB-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image without Crypto)
- S45ESK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support)
- S45LB-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (LAN Base image)
- S45LBK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (LAN Base image with 3DES)
- S45IPBU-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (IP Base Upgrade image)
- S45IPBUK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE (IP Base Upgrade image with 3DES)
- S45EES-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image)
- S45EESK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image with 3DES)
- S45EIPB-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Supervisor Engine 6-E and 6L-E (IP Base image)
- S45EIPBK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6-E and 6L-E (IP Base image with 3DES)
- S45ELB-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6L-E (LAN Base image)
- S45ELBK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6L-E (LAN Base image with 3DES)
- S45EIPBU-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6L-E (IP Base Upgrade image)

- S45EIPBUK9-12253SG - Cisco IOS Software for the Cisco Catalyst 4500 Series Supervisor Engine 6L-E (IP Base Upgrade image with 3DES)
- S45ELB-12252X0 - Cisco IOS software for the Catalyst 4500 Sup 6L-E (LAN Base, without crypto)
- S45ELBK9-12252X0 Cisco IOS software for the Catalyst 4500 Sup 6L-E (LAN Base image with Triple Data Encryption Standard(3DES))
- S45EIPB-12252X0 Cisco IOS software for the Catalyst 4500 Sup 6L-E (IP Base image without Crypto)
- S45EIPBK9-12252X0 Cisco IOS software for the Catalyst 4500 Sup 6L-E (IP Base image with Triple Data Encryption Standard(3DES))
- S45EIPBU-12252X0 Cisco IOS software for the Catalyst 4500 Sup 6L-E (IP upgrade image without Crypto)
- S45EIPBUK9-12252X0 Cisco IOS software for the Catalyst 4500 Sup 6L-E (IP upgrade image with Triple Data Encryption Standard(3DES))
- S45IPB-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image, without Crypto) (cat4500-ipbase-mz)
- S45IPBK9-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support, without Crypto) (cat4500-entservices-mz)
- S45ESK9-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45EIPB-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45EIPBK9-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)
- S45EES-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45EESK9-12252SG-Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45IPB-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image, without Crypto) (cat4500-ipbase-mz)
- S45IPBK9-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support, without Crypto) (cat4500-entservices-mz)
- S45ESK9-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45EIPB-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45EIPBK9-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)

- S45EES-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45EESK9-12250SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45IPB-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image, without Crypto) (cat4500-ipbase-mz)
- S45IPBK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support, without Crypto) (cat4500-entservices-mz)
- S45ESK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45EIPB-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45IPBK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)
- S45EES-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45EESK9-12246SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45IPB-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image, without Crypto) (cat4500-ipbase-mz)
- S45IPBK9-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support, without Crypto) (cat4500-entservices-mz)
- S45ESK9-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45EIPB-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45IPBK9-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)
- S45EES-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45EESK9-12244SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500-ipbasek9-mz)
- S45IPB-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image, without Crypto) (cat4500-ipbase-mz)
- S45IPBK9-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support, without Crypto) (cat4500-entservices-mz)

- S45ESK9-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45EIPB-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image)
- S45IPBK9-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (IP Base Image with 3DES) (cat4500-ipbasek9-mz)
- S45EES-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services image) (cat4500e-entservices-mz)
- S45EESK9-12240SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engine 6-E (Enterprise Services with 3DES image) (cat4500-entservicesk9-mz)

Catalyst 4500 Series Switch Cisco IOS Release Strategy

Cisco IOS Release 12.2SG train offers the latest features for the Catalyst 4500 Series supervisor engines. Customers with Catalyst 4500 Series supervisor engines who need the latest hardware support and software features should migrate to Cisco IOS Release 12.2(54)SG.



Note

As part of the Cisco IOS Reformation effort, Cisco IOS Releases 12.2EW and 12.2SG are the same release train with a name change.

Catalyst 4500 Series has three maintenance trains. The Cisco IOS Release 12.2(31)SGA train is the longest living train. Currently, the Cisco IOS Release 12.2(31)SGA8 is the recommended release for customers who require a release with a maintenance train. The Cisco IOS Release 12.2(53)SG is the latest maintenance train and includes the most recent features including support for the WS-X45-Sup6L-E supervisor engine and OSPF for routed Access.

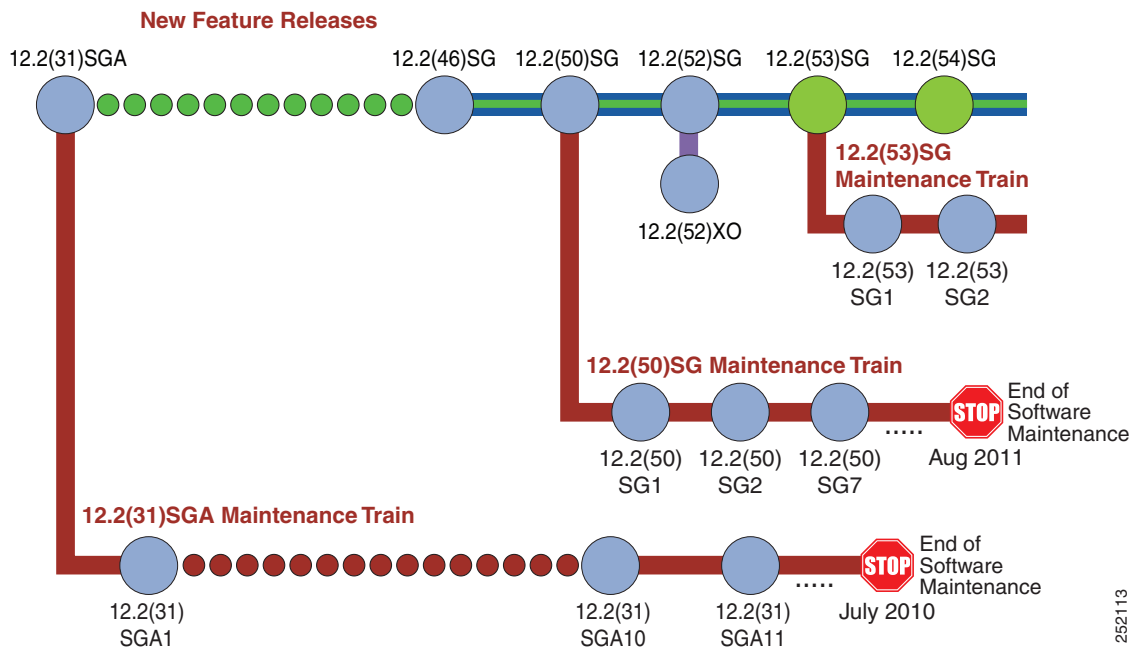
For more information on the Catalyst 4500 series switches, visit the following URL:

<http://www.cisco.com/go/cat4500/docs>

Cisco IOS Software Migration Guide

Figure 1 displays the two active, 12.2(31)SGA and 12.2(50)SG, and newly introduced 12.2(53)SG extended maintenance trains.

Figure 1 *Software Release Strategy for the Catalyst 4500 Series Switch*



Summary of Migration Plan

- Customers requiring the latest Cisco Catalyst 4500 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(54)SG.
- Cisco IOS Software Release 12.2(31)SGA and 12.2(50)SG will continue offering maintenance releases. The latest release from the 12.2(31)SGA maintenance train is 12.2(31)SGA10. The latest release from the 12.2(50)SG maintenance train is 12.2(50)SG4

Support

Support for Cisco IOS Software Release 12.2(54)SG follows the standard Cisco Systems® support policy, available at

http://www.cisco.com/en/US/products/products_end-of-life_policy.html

System Requirements

This section describes the system requirements:

- [Supported Hardware on Catalyst 4500 Series Switch, page 13](#)
- [Supported Features on the Catalyst 4500 Series Switch, page 19](#)
- [Unsupported Features, page 29](#)

Supported Hardware on Catalyst 4500 Series Switch

Table 2 lists the hardware supported on the Catalyst 4500 Series Switch.

Table 2 **Supported Hardware**

Product Number (append with “=” for spares)	Product Description	Software Release
		Minimum
Supervisor Engines		
WS-X4013+=	Catalyst 4500 series switch Supervisor Engine II-Plus Note This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.1(19)EW
WS-X4013+TS	Catalyst 4500 series switch Supervisor Engine II-Plus-TS Note This engine is supported only on 3 slot chassis.	12.2(20)EWA
WS-X4013+10GE	Catalyst 4500 series switch Supervisor Engine II-Plus-10GE Note This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.2(25)SG
WS-X4515=	Catalyst 4500 series switch Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R series switch Redundant Supervisor Engine IV	12.1(12c)EW
WS-X4516=	Catalyst 4500 series switch Supervisor Engine V	12.2(18)EW
WS-X4516/2=	Catalyst 4507R series switch Redundant Supervisor Engine V	12.2(18)EW
WS-X4516-10GE=	Catalyst 4500 series switch Supervisor Engine V-10GE	12.2(25)EW
WS-X45-Sup6-E	Catalyst 4500 E-series switch Supervisor Engine 6-E Note This engine is supported on legacy and E-series chassis.	12.2(40)SG
WS-X45-Sup6L-E	Catalyst 4500 E-series switch Supervisor Engine 6L-E Note This engine is supported on legacy and E-series 3,6, and 7 slot chassis.	12.2(52)XO
Gigabit Ethernet Switching Modules		
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module	12.1(19)EW
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module	12.1(8a)EW
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module	12.1(8a)EW
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module	12.1(8a)EW
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module	12.1(8a)EW
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module	12.2(20)EW

Table 2 **Supported Hardware (continued)**

Product Number (append with “=” for spares)	Product Description	Software Release
		Minimum
WS-X4506-GB-T	6-port Alternately-Wired 10/100/1000BASE-T Catalyst 4500 series Power over Ethernet (PoE) 802.3af or 1000BASE-X SFP	12.2(20)EWA
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module	12.1(19)EW
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card	12.2(50)SG
WS-X4624-SFP-E	Non-blocking 24-port 1000BASEX (small form factor pluggable) module	12.2(44)SG
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
Fast Ethernet Switching Modules		
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module	12.1(13)EW
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module	12.2(18)EW
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module	12.2(25)SG
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card	12.1(8a)EW
Ethernet/Fast Ethernet (10/100) Switching Modules		
WS-X4124-RJ45	24-port 10/100 RJ-45 module	12.2(20)EW
WS-X4148-RJ	48-port 10/100 RJ-45 switching module	12.1(8a)EW
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module	12.1(8a)EW
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module	12.1(8a)EW for data support 12.1(11b)EW for data and inline power support
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(20)EW
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco	12.2(18)EW

Table 2 **Supported Hardware (continued)**

Product Number (append with “=” for spares)	Product Description	Software Release
		Minimum
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module	12.1(8a)EW
Other Modules		
MEM-C4K-FLD64M	Catalyst 4500 series switch CompactFlash, 64 MB Option	12.1(8a)EW
MEM-C4K-FLD128M	Catalyst 4500 series switch CompactFlash, 128 MB Option	12.1(8a)EW
WS-F4531	Catalyst 4500 series switch NetFlow Services Card on Catalyst 4500 series switch Supervisor Engines IV and V	12.1(13)EW
WS-X4590=	Catalyst 4500 series switch Fabric Redundancy Modules	12.2(18)EW
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)	12.2(25)EW
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM	12.1(19)EW
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)	12.1(12c)EW
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)	12.2(25)EWA5
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502	12.1(19)EW
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply	12.1(19)EW
PWR-C45-6000ACV	Catalyst 4500 Series Switch 6000 W AC power supply	12.2(53)SG

For Catalyst 4500 transceiver module compatibility information, see the url:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Table 3 briefly describes the four chassis in the Catalyst 4500 Series Switch. For the chassis listed in the table, refer to Table 6 on page 18 for software release information.

Table 3 Chassis Description for the Catalyst 4500 Series Switch

Product Number (append with “=” for spares)	Description of Modular Chassis
WS-C4503	<p>Catalyst 4503 chassis includes these components:</p> <ul style="list-style-type: none"> • 3 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus-TS, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4506	<p>Catalyst 4506 chassis includes these components:</p> <ul style="list-style-type: none"> • 6 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4507R	<p>Catalyst 4507R chassis includes these components:</p> <ul style="list-style-type: none"> • 7 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine II-Plus-10GE, and Supervisor Engine II-Plus
WS-C4510R	<p>Catalyst 4510R chassis includes these components:</p> <ul style="list-style-type: none"> • 10 slots; slot 10 accepts only the Catalyst 4500 series 2-port Gigabit Ethernet line card (WS-X4302-GB with Supervisor Engine V) <p>Note The Supervisor Engine V-10GE does not have this restriction.</p> <ul style="list-style-type: none"> • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE and Supervisor Engine V

Table 4 *DOM Support on the Catalyst 4500 Series Switch*

Transceiver Module	Support in Software Since...
CWDM- SFP- <i>xx</i>	12.2(20)EWA
DWDM-GBIC- <i>xx</i>	12.1(19)EW
DWDM-SFP	12.2(37)SG
DWDM-X2- <i>xx</i>	12.2(50)SG
GLC-BX-D	12.2(20)EWA
GLC-BX-U	12.2(20)EWA
SFP-10G-SR	12.2(54)SG
SFP-10G-LR	12.2(54)SG
SFP-10G-LRM	12.2(54)SG

Supported Hardware on Catalyst 4500 E-Series Switch

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(54)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis. A brief list of primary E-Series hardware supported on Catalyst 4500 series switch ([Table 5](#)).

Table 5 *Supported E-Series Hardware*

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500 E-Series 3-Slot Chassis <ul style="list-style-type: none"> Fan tray No Power Supply
WS-C4506-E	Cisco Catalyst 4500 E-Series 6-Slot Chassis <ul style="list-style-type: none"> Fan tray No Power Supply
WS-C4507R-E	Cisco Catalyst 4500 E-Series 7-Slot Chassis <ul style="list-style-type: none"> Fan tray No Power Supply Redundant supervisor engine capability
WS-C4507R+E	Cisco Catalyst 4500 E-Series 7-Slot 48 GB-ready Chassis <ul style="list-style-type: none"> Fan tray No Power Supply Redundant supervisor engine capability

Table 5 **Supported E-Series Hardware**

Product Number	Description
WS-C4510R-E	Cisco Catalyst 4500 E-Series 10-Slot Chassis <ul style="list-style-type: none"> Fan tray No Power Supply Redundant supervisor engine capability All port card slots support 6, 24, and 48Gbps when used with Supervisor Engine 7-E. Slots 8, 9, and 10 are limited to 6Gbps when used with a Supervisor Engine 6-E.
WS-C4510R+E	Cisco Catalyst 4500 E-Series 10-Slot 48 GB-ready Chassis <ul style="list-style-type: none"> Fan tray No Power Supply Redundant supervisor engine capability You cannot place a linecard with a backplane traffic capacity exceeding 6Gbps in slots 8, 9 and 10 of a Catalyst 4510R+E chassis when used with a Supervisor Engine 6-E.
WS-X45-Sup6-E	Cisco Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ TwinGig
WS-X45-Sup6L-E	Cisco Catalyst 4500 E-Series Sup 6L-E
WS-X4624-SFP-E	Cisco Catalyst 4500 E-series 24-Port 1000BaseX (small form factor pluggable) module
WS-X4648-RJ45V-E	Cisco Catalyst 4500 E-Series 48-Port PoE 802.3af 10/100/1000(RJ45)
WS-X4648-RJ45V+E	Cisco Catalyst 4500 E-Series 48-Port Premium PoE 10/100/1000
WS-X4606-X2-E	Cisco Catalyst 4500 E-Series 6-Port 10GbE (X2) w/ TwinGig
WS-X4648-RJ45-E	Cisco Catalyst 4500 E-Series 48-Port 10/100/1000(RJ45)

Table 6 outlines the chassis and supervisor engine compatibility.
(M=Minimum release, R=Recommended release)

Table 6 **Chassis and Supervisor Compatibility**

Chassis	Sup II+	Sup II+TS	Sup II+10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4506-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4507R-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO

Table 6 Chassis and Supervisor Compatibility

Chassis	Sup II+	Sup II+TS	Sup II+10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4507R+E	M: 12.2(54)SG R: 12.2(54)SG		M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG
WS-C4510R-E					M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	
WS-C4510R+E					M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	

Supported Features on the Catalyst 4500 Series Switch

Table 7 lists the Cisco IOS software features for the Catalyst 4500 Series Switch.

Table 7 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Layer 2 Switching Features

Storm Control

Storm Control: Per-Port Multicast Suppression (Sup 6-E only)

Multicast Storm Control¹

IP Source Guard

IP Source Guard for Static Hosts

PVRST+

Layer 2 protocol tunneling

Layer 2 transparent bridging²

Layer 2 MAC³ learning, aging, and switching by software

Unicast MAC address filtering

VMPS⁴ Client

Layer 2 hardware forwarding up to 102 Mpps

Layer 2 Control Policing (Sup 6-E and Sup 6L-E only)

Layer 2 switch ports and VLAN trunks

Spanning-Tree Protocol (IEEE 802.1D) per VLAN

802.1s and 802.1w

Layer 2 traceroute

Unidirectional Ethernet port

Per-VLAN spanning tree (PVST) and PVST+

Spanning-tree root guard

Spanning-tree Loop guard and PortFast BPDU Filtering

Table 7 *Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch*

Support for 9216 byte frames
Port security on PVLANS
Private VLANs
Private VLAN DHCP snooping
Private VLAN promiscuous trunk
Private VLAN trunks ⁵
Community PVLANS
ISL ⁶ -based VLAN encapsulation (excluding blocking ports on WS-X4418-GB and WS-X4412-2GB-T) ⁷
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
VTP v3
No. of VLAN support per switch: 2048 (for LAN Base), 4096 (for IP Base)
Unidirectional link detection (UDLD) and aggressive UDLD
Sub-second UDLD (Fast UDLD)
SNMP V3 support for Bridge-MIB with VLAN indexing
Resilient Ethernet Protocol
Ethernet CFM
Ethernet OAM Protocol
Layer 3 Routing, Switching, and Forwarding
802.1Q Tunneling (Q in Q) ⁸
Pragmatic General Multicast
ANCP Client ⁹
PIM-SSM mapping
Bidirectional PIM ¹⁰
Auto RP Listener
IP and IP multicast routing and switching between Ethernet ports
IP Multicast Load Splitting (Equal Cost Multipath (ECMP) using S, G and Next-hop)
Static IP routing
Classless routing ¹¹
PBR ¹²
Dynamic Buffer Limiting
Selective Dynamic Buffer Limiting
QoS-based forwarding based on IP precedence
Trusted boundary
Cisco Modular QoS Command-Line Interface (Sup 6-E and Sup 6L-E only)
Auto QoS

Table 7 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Match CoS for non-IPv4 traffic
IPv6 Forwarding in Hardware (Sup 6-E and Sup 6L-E only)
CoS Mutation
CEF ¹³ load balancing
uRPF ¹⁴ (Sup 6-E and Sup 6L-E only)
Hardware-based IP CEF routing at 48 Mpps
Up to 128,000 IP routes
Up to 32,000 IP host entries (Layer 3 adjacencies)
Up to 16,000 IP multicast route entries
Multicast flooding suppression for STP changes
Software routing of IPX, AppleTalk, and IPv6.
IGMPv1, IGMPv2, and IGMPv3 (Full Support)
IGMP Querier
VRF-lite
Multicast VRF-lite ¹⁵
VRF-aware IP services
VRF-aware TACACS+
Route Leaking ¹⁶
IP Unnumbered
SVI Autostate Exclude
Supported Protocols
IS-IS ¹⁷
DTP ¹⁸
RIP ¹⁹ and RIP II
EIGRP ²⁰
EIGRP IPv6 (Sup 6-E and Sup 6L-E only)
OSPF ²¹
OSPF for Routed Access ²²
BGP4 ²³
BGP route-map Continue
BGP Neighbor Policy
MBGP ²⁴
MSDP ²⁵
ICMP ²⁶ Router Discovery Protocol
PIM ²⁷ —sparse and dense mode
Static routes
Classless interdomain routing (CIDR)

Table 7 *Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch*

DVMRP ²⁸
SSM
NTP ²⁹
WCCP version 2 Layer 2 Redirection
VRRP ³⁰
SCP ³¹
GLBP ³²
EtherChannel Features
Cisco EtherChannel technology - 10/100/1000 Mbps, 10 Gbps
Load balancing for routed traffic, based on source and destination IP addresses
Load sharing for bridged traffic based on MAC addresses
ISL on all EtherChannels
IEEE 802.1Q on all EtherChannels
Bundling of up to eight Ethernet ports
Up to 64 active Ethernet port channels
Trunk Port Security over EtherChannel
Link State Tracking
Additional Protocols and Features
Link Layer Discovery Protocol (LLDP)
Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED)
PoEP via LLDP
DSCP/CoS via LLDP
Routed Jumbo Frame support
SPAN CPU port mirroring
SPAN packet-type filtering
SPAN destination in-packets option
SPAN ACL filtering
RSPAN
Enhanced VLAN statistics
Netflow version 8
NetFlow Statistics Collection
NetFlow Statistics Export Version 1 and Version 5
NetFlow Bridged IP Flow
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
Cisco Discovery Protocol (CDP)

Table 7 *Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch*

CDP 2nd Port Status TLV
MAC Address-Table Move Update
Flex Link Bi-directional Fast Convergence
Flex Link VLAN Load-Balancing
Flex Links
Flex Links Interface Preemption
802.1ab Link Layer Discovery Protocol (LLDP)
802.1ab LLDP Media Discovery (LLDP-MED)
Network Mobility Services Protocol
Selecting Mode of Capturing Control Packets (Not supported on Sup 6-E)
Sticky port security
Trunk port security
Voice VLAN Sticky port security
Cisco Group Management Protocol (CGMP) server support
HSRP ³³ over Ethernet, EtherChannels - 10/100/1000Mbps, 10 Gbps
HSRP v2 for IPv4
HSRP v2 for IPv6
IGMP snooping version1, version 2, and version 3 (Full Support)
IGMP filtering
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2 ³⁴
Inline power preallocation
show interface capabilities command
IfIndex persistence
UDLR ³⁵
Enhanced SNMP MIB support
SNMP ³⁶ version 1, version 2, and version 3
SNMP version 3 (with encryption)
IPv6 Multicast Listener Discovery Snooping (Sup 6-E and 6L-E only)
IPv6 PACL (Sup 6-E and 6L-E only)
IPv6 RA Guard (Sup 6-E and 6L-E only)
IPv6 Interface Statistics (Sup 6-E and 6L-E only)
DHCP server and relay-agent
DHCP snooping
DHCP client autoconfiguration
DHCP Option 82 Pass Through

Table 7 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

DHCP Relay Agent for IPv6 ³⁷
802.1X Multiple Domain Authentication and Multiple Authorization
802.1X with ACL Assignment and Redirect URLs
802.1X with per-user ACL and Filter-ID ACL
RADIUS-Provided Session Timeouts
RADIUS CoA
MAC Move and Replace
802.1X with Guest VLANs
802.1X port-based authentication
802.1X with port security
802.1X accounting
802.1X with voice VLAN ID
802.1X private VLAN assignment
802.1X private guest VLAN
802.1X RADIUS-supplied session timeout
802.1X authentication failure VLAN
802.1X MAC Authentication Bypass
802.1X Inaccessible Authentication Bypass
802.1X with User Distribution
802.1X Unidirectional Controlled Port
802.1X MDA with Voice Assignment
Cisco TrustSec SGT Exchange Protocol (SXP) IPv4
Flexible Authentication Sequencing
Multi-Authentication
Open Authentication
Web Authentication
Local Web Authentication (EPM syslog and Common session ID)
PPPoE Intermediate Agent ³⁸
Cisco NAC ³⁹ Layer 2 802.1X
Port flood blocking
Router standard and extended ACLs ⁴⁰ on all ports with no performance penalty
Identity 4.1 ACL Policy Enforcement ⁴¹
Identity 4.1 Network Edge Access Topology
Extended IPX ACL
VLAN ACL
PACL ⁴²
Time-based ACL

Table 7 *Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch*

Downloadable ACLs
Control Plane Policing
Two-Rate Three-Color Policing (Sup 6-E and Sup 6L-E only)
Local Proxy ARP
Dynamic ARP Inspection on PVLANS
Dynamic ARP Inspection
Dynamic Multi-Protocol Ternary Content Addressable Memory (Sup 6-E and Sup 6L-E only)
Per-port QoS ⁴³ rate-limiting and shaping
QoS for IPv6
Per-port Per-VLAN QoS
Per-VLAN CTI
ARP QoS (Sup 6-E and Sup 6L-E only)
Inline power support for Cisco IP phones
PoE ⁴⁴
Energy Wise
Enhanced Power over Ethernet Support (Sup 6-E and Sup 6L-E only)
Power redundancy
RPR ⁴⁵
SSO ⁴⁶
SSO Aware HSRP
SSO support for routed ports
Non-stop Forwarding Awareness
Non-stop Forwarding Awareness for EIGRP-stub in IP base for all supervisor engines
Non-stop Forwarding with Stateful Switchover
ISSU ⁴⁷
MAC Address Notification
Combined Mode Power Resiliency
SmartPort macros
AutoSmartPort macros
Forced 10/100 Auto Negotiation
802.1s standards compliance
IS-IS MIB
OSPF and EIGRP Fast Convergence ⁴⁸
Time Domain Reflectometry
CNA ⁴⁹
CLI to turn off Auto MDIX ⁵⁰
Logging redirection

Table 7 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Service-Aware Resource Allocation (Sup 6-E and Sup 6L-E only)
TwinGig Converter Module (Sup 6-E and 6L-E only)
FAT File System (Sup 6-E and Sup 6L-E only)
High Availability: 2+2 10GE or 4+4 1GE active uplinks (Sup 6-E only)
EEM ⁵¹
EEM with ISSU
VSS client with PagP+
IP/SLA ⁵²
Embedded management ⁵³
MAC notify MIB
Eight configurable queues per port (Sup 6-E and Sup 6L-E only)
X2 Link Debounce Timer
IP SLA
Enhanced Object Tracking subfeatures: <ul style="list-style-type: none"> • HSRP with EOT • VRRP with EOT • GLBP with EOT • IP SLA with EOT • Reliable Backup Static Routing with EOT
Management port
Management Port Features with IPv6
Inactivity Timer
OBFL ⁵⁴
boot config command
Crashdump enhancement
Unicast MAC filtering
Smart Call Home
DHCPv6 Ethernet Remote ID option
DHCPv6 Relay - Persistent Interface ID option DHCPv6 Relay Agent notification for Prefix Delegation
PIM SSM Mapping
VRF lite NSF support with routing protocols OSPF/EIGRP/BG
PIM Accept Register - Rogue Multicast Server Protection ⁵⁵
Configuration Rollback
Archiving crashfile information
Per-VLAN Learning
XML Programmatic Interface

Table 7 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

VLAN Mapping (VLAN Translation)
GOLD Online Diagnostics (Sup 6-E and 6L-E only)
IPSG for Static Hosts
Layer Control Packet
Fa1 interface (Ethernet management port) ⁵⁶
<ol style="list-style-type: none"> 1. Requires the Catalyst 4500 series switch Supervisor Engine V 2. Hardware-based transparent bridging within a VLAN 3. MAC = Media Access Control 4. VMPS = VLAN Management Policy Server 5. Only Supervisor Engine 6-E 6. ISL = Inter-Switch Link 7. Ports 3 thru 18 on the WS-X4418-GB and ports 1 thru 12 on the WS-X4412-2GB 8. Requires the Catalyst 4500 series switch Supervisor Engine V 9. not supported on E-Series Supervisor Engine 6-E 10. Only Supervisor Engine 6-E 11. The ip classless command is not supported as classless routing is enabled by default. 12. PBR = policy-based routing 13. CEF = Cisco Express Forwarding 14. uRPF = Unicast Reverse Path Forwarding 15. Only Supervisor Engine 6-E 16. Route Leaking from a global routing table into a VRF and Route Leaking from a VRF into a global routing table 17. IS-IS = Intermediate System to Intermediate System 18. DTP = Dynamic Trunking Protocol 19. RIP = Routing Information Protocol 20. EIGRP = Enhanced Interior Gateway Routing Protocol 21. OSPF = Open Shortest Path First 22. Support for Supervisor Engine 6-E and Supervisor Engine 6L-E only 23. BGP4 = Border Gateway Protocol 4 24. MBGP = Multicast Border Gateway Protocol 25. MSDP = Multicast Source Discovery Protocol 26. ICMP = Internet Control Message Protocol 27. PIM = Protocol Independent Multicast 28. DVMRP = Distance Vector Multicast Routing Protocol 29. NTP = Network Time Protocol 30. VRRP = Virtual Router Redundancy Protocol 31. SCP = Secure Copy Protocol 32. GLBP = Gateway Load Balancing Protocol 33. HSRP = Hot Standby Router Protocol 34. SSH = Secure Shell Protocol 35. UDLR = Unidirectional Link Routing 36. SNMP = Simple Network Management Protocol 37. only Sup 6-E and 6L-E 38. not supported on E-Series Supervisor Engine 6-E 39. NAC = Network Admission Control 40. ACLs = Access Control Lists 41. filter-ID and per-user ACL 42. PACL = Port Access Control List

43. QoS = Quality of Service
44. PoE = Power over Ethernet
45. RPR = Supervisor engine redundancy
46. SSO = Stateful switchover (includes Stateful IGMP Snooping and Stateful DHCP Snooping)
47. ISSU = In Service Software Upgrade Process
48. The Catalyst 4500 series switch supports Fast Hellos, ISPF, and LSA Throttling.
49. CNA = Cisco Network Assistant; Minimum CNA release that supports Releases 12.2(25)EW is 1.0(2). Minimum CNA release that supports Release 12.2(20)EWA is 1.0(1).
50. On supported linecards: WS-X4124-RJ45, WS-X4148-RJ (and WS-X4232-GB-RJ) with hardware revision 3.0 or higher
51. EEM = Embedded Event anager
52. Includes HTTPS-HTTP with SSL 3.0, CEF-MIB, Embedded Syslog Manage, ...
53. Includes SNMP over IPv6, SYSLOG, HTTP over IPv6.
54. OBFL = On Board Failure Logging; Supverisor Engine 6-E only
55. The route-map keyword is not supported.
56. Available starting with Cisco IOS Release 12.2(46)SG

Features Unique to Supervisor Engines 6-E and 6L-E

With Cisco IOS Release 12.2(54)SG, the following features are available only with Supervisor Engine 6-E and Supervisor Engine 6L-E:

- IPv6
 - IPv6 Addressing Architecture
 - CDP IPv6 Address Family
 - DNS resolver for AAAA over an IPv4 transport
 - DNS resolver for AAAA over an IPv6 transport
 - Extended ACL
 - Hop-by-Hop option header
 - ICMP Rate Limiting
 - ICMPv6
 - ICMPv6 Redirect
 - IPv6 over IEEE 802.1Q
 - ISATAP (supported in software only)
 - Loopback
 - MLD Snooping (supported in software and hardware on Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Catalyst 6L-E)
 - MLDv1/v2
 - MTU Path Discovery for IPv6
 - OSPFv3
 - RIPng
 - EIGRPv6
 - PACL
 - RA Guard
 - IPv6 Interface Statistics

- FAT filesystem
- PIM (SM, DM, SDM)
- QoS
 - Two Rate three Color Policing
 - Table map support for marking
 - Class based queuing actions (shaping/bandwidth/queue-limit/dbl/strict priority)
- Voltage Margining CLI
- QoS for IPv6
- ARP QoS

Unsupported Features

For all Supervisor Engines (II-Plus thru 6-E), the following features are not supported in Cisco IOS Release 12.2(54)SG for the Catalyst 4500 series switches:

- The following ACL types:
 - Standard Xerox Network System (XNS) access list
 - Extended XNS access list
 - DECnet access list
 - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- CEF Accounting
- Cisco IOS software IPX ACLs:
 - <1200-1299> IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- Kerberos support for access control
- LLDP HA
- Lock and key
- NAT-PT for IPv6
- NetFlow per-VRF
- PBR with Multiple Tracking Options
- QoS for IPv6 traffic (only supported on Supervisor 6)

- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- WCCP version 1
- CFM CoS
- PBR with EOT

New and Changed Information

These sections describe the new and changed information for the Catalyst 4500 series switch running Cisco IOS software:

- [New Hardware Features in Release 12.2\(54\)SG1, page 31](#)
- [New Software Features in Release 12.2\(54\)SG1, page 31](#)
- [New Hardware Features in Release 12.2\(54\)SG, page 31](#)
- [New Software Features in Release 12.2\(54\)SG, page 31](#)
- [New Hardware Features in Release 12.2\(53\)SG3, page 33](#)
- [New Software Features in Release 12.2\(53\)SG3, page 33](#)
- [New Hardware Features in Release 12.2\(53\)SG3, page 33](#)
- [New Software Features in Release 12.2\(53\)SG3, page 33](#)
- [New Hardware Features in Release 12.2\(53\)SG2, page 33](#)
- [New Software Features in Release 12.2\(53\)SG2, page 33](#)
- [New Hardware Features in Release 12.2\(53\)SG1, page 34](#)
- [New Software Features in Release 12.2\(53\)SG1, page 34](#)
- [New Hardware Features in Release 12.2\(53\)SG, page 34](#)
- [New Software Features in Release 12.2\(53\)SG, page 34](#)
- [New Hardware Features in Release 12.2\(52\)XO, page 35](#)
- [New Software Features in Release 12.2\(52\)XO, page 35](#)
- [New Hardware Features in Release 12.2\(52\)SG, page 36](#)
- [New Software Features in Release 12.2\(52\)SG, page 36](#)
- [New Hardware Features in Release 12.2\(50\)SG1, page 38](#)
- [New Software Features in Release 12.2\(50\)SG1, page 38](#)
- [New Hardware Features in Release 12.2\(50\)SG, page 38](#)
- [New Software Features in Release 12.2\(50\)SG, page 38](#)
- [New Hardware Features in Release 12.2\(46\)SG, page 40](#)
- [New Software Features in Release 12.2\(46\)SG, page 40](#)
- [New Hardware Features in Release 12.2\(44\)SG, page 41](#)
- [New Software Features in Release 12.2\(44\)SG, page 41](#)
- [New Hardware Features in Release 12.2\(40\)SG, page 42](#)

- [New Software Features in Release 12.2\(40\)SG, page 43](#)

New Hardware Features in Release 12.2(54)SG1

Release 12.2(54)SG1 provides the following new hardware on the Catalyst 4500 series switch:

- Catalyst 4948E-F—The Catalyst 4948E and Catalyst 4948E-F share the same internal hardware and software. The Catalyst 4948E draws cold air into the port side and exhausts hot air on the power supply side. The Catalyst 4948E-F draws cold air at the power supply side and exhaust hot air on the port side. This is the only difference between the Catalyst 4948E and the Catalyst 4948E-F.

New Software Features in Release 12.2(54)SG1

Release 12.2(54)SG provide no new software features on the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(54)SG

Release 12.2(54)SG provides the following new hardware on the Catalyst 4500 series switch:

- SFP-10G-LRM
- WS-C4507R+E
- WS-C4510R+E
- Digital Optical Monitoring (DOM) support on all 10GE interfaces
- CVR-X2-SFP10G (support introduced on Supervisor Engines II+ through V-10GE)

New Software Features in Release 12.2(54)SG

Release 12.2(54)SG provides the following new software features on the Catalyst 4500 series switch:

- 802.1X with User Distribution ("Configuring 802.1X Port-Based Authentication" chapter)
- Auto SmartPort ("Configuring Auto SmartPort Macros" chapter)
- DSCP/CoS via LLDP ("Configuring LLDP, LLDP-MED, and Location Service" chapter)
- EEM: Embedded Event Manager 3.2

For details, refer to the URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_12eem.html

- EIGRP Service Advertisement Framework

For details refer to the URL:

http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html

- EnergyWise 2.0

For details refer to the URL:

http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

- GOLD Online Diagnostics ("Performing Diagnostics" chapter; Supervisor Engine 6-E only)
- Identity 4.1 ACL Policy Enhancements ("Configuring Network Security with ACLs" chapter)
- Identity 4.1 Network Edge Access Topology ("Configuring 802.1X Port-Based Authentication" chapter)
- IPSG for Static Hosts (Refer to the Cisco IOS library)
- IPv6 PACL ("Configuring Network Security with ACLs" chapter; Supervisor Engine 6-E only)
- IPv6 RA Guard ("Configuring Network Security with ACLs" chapter; Supervisor Engine 6-E only)
- IPv6 Interface Statistics ("Configuring Layer 3 Interfaces" chapter; Supervisor Engine 6-E only)
- IS-IS for IPv4 and IPv6, extended to Supervisor Engine 6-E (Refer to the Cisco IOS library)
- Layer Control Packet (extended to Supervisor 6)
- Link State Tracking ("Configuring EtherChannel and Link State Tracking" chapter)
- MAC move and replace ("Administering the Switch" chapter)
- Per-VLAN Learning ("Administering the Switch" chapter)
- PoEP via LLDP ("Configuring LLDP, LLDP-MED, and Location Service" chapter)
- RADIUS CoA ("Configuring 802.1X Port-Based Authentication" chapter)
- Sub-second UDLD (Configuring UDLD" chapter)
- VLAN Translation ("Configuring 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling" chapter; Supervisor Engine 6-E only)
- VRF-aware TACACS+ ("Configuring VRF-lite" chapter)
- XML Programmatic Interface (Refer to the Cisco IOS library)

For details refer to the URL:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_xmlpi_v1.html

New Hardware Features in Release 12.2(53)SG6

Release 12.2(53)SG6 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(53)SG6

Release 12.2(53)SG6 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG5

Release 12.2(53)SG5 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(53)SG5

Release 12.2(53)SG5 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG4

Release 12.2(53)SG4 provides the following new hardware on the Catalyst 4500 series switch:

- WS-C4507-R+E
- WS-C4510-R+E

New Software Features in Release 12.2(53)SG4

Release 12.2(53)SG4 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG3

Release 12.2(53)SG3 provides the following new hardware on the Catalyst 4500 series switch:



Note

This set of optics is not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG. However, the same set of optics is supported on Cisco IOS Release 15.0(2)SG and Cisco IOS XE Release 3.2.0(SG).

- DWDM-SFP-6141
- DWDM-SFP-5736
- DWDM-SFP-5332
- DWDM-SFP-4931
- DWDM-SFP-4532
- DWDM-SFP-4134
- DWDM-SFP-3739
- DWDM-SFP-3346

New Software Features in Release 12.2(53)SG3

Release 12.2(53)SG3 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG2

Release 12.2(53)SG2 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(53)SG2

Release 12.2(53)SG2 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG1

Release 12.2(53)SG1 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(53)SG1

Release 12.2(53)SG1 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(53)SG

Release 12.2(53)SG does not provide any new hardware for the Catalyst 4500 series switch. However, it does integrate Supervisor Engine 6L-E, introduced in 12.2(52)XO.

New Software Features in Release 12.2(53)SG

Release 12.2(53)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

- IP Multicast Load Splitting (Equal Cost Multipath (ECMP) using S, G and Next-hop)
- OSPF for Routed Access (Supervisor Engine 6-E and Supervisor Engine 6L-E)

OSPF for Routed Access is designed specifically to enable customers to extend Layer 3 routing capabilities to the access or Wiring Closet.



Note

OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.

With the typical topology (hub and spoke) in a campus environment, where the wiring closets (spokes) are connected to the distribution switch (hub) forwarding all nonlocal traffic to the distribution layer, the wiring closet switch need not hold a complete routing table. A best practice design, where the distribution switch sends a default route to the wiring closet switch to reach inter-area and external routes (OSPF stub or totally stub area configuration) should be used when OSPF for Routed Access is used in the wiring closet.

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/54sg/configuration/guide/automacr.html>

The OSPF for Routed Access feature adheres to the following software restrictions:

- Limit the number of OSPF instances to one on OSPFv2 and one on OSPFv3.
- Limit number of dynamic routes learned through platform dependant work to 200.

Refer to the following link for more details:

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html>

With Cisco IOS Release 12.2(53)SG, the IP Base image supports OSPF for routed access. The Enterprise Services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions. Additionally, Enterprise Services is required to enable the VRF-lite feature.

New Hardware Features in Release 12.2(52)XO

Release 12.2(52)XO provides the following new hardware for the Catalyst 4500 series switch:

- WS-X45-Sup6L-E, Catalyst 4500 E-series switch Supervisor Engine 6L-E
- PWR-C45-6000ACV, Catalyst 4500 series switch 6000 Watt AC power supply



Note Only supported on 3, 6, and 7 slot chassis and IP LAN and IP BASE images

New Software Features in Release 12.2(52)XO



Note

This release is equivalent in functionality to 12.2(52)SG, but adds support for the new Sup6L-E supervisor. The only supervisor engine it supports is Supervisor Engine 6L-E; for all other supervisor engines, use 12.2(52)SG instead.

Release 12.2(52)XO provides the following Cisco IOS software features for the Catalyst 4500 series switch:

- EnergyWise
- Switch and IP Phone interaction for security features
 - Port Security
 - DHCP Snooping
 - Dynamic ARP Inspection
 - BPDU Guard
- Network Mobility Services Protocol
- Identity ACL Policy Enforcement Enhancement
 - Filter-ID
 - Per-user ACL
- Smart Call Home*
- Management Port Features with IPv6
- Local WebAuth Enhancement
- MDA with Voice Assignment
- HSRP v2 for IPv4
- HSRP v2 or IPv6
- DHCPv6 Enhancements
 - DHCPv6 Ethernet Remote ID option
 - DHCPv6 Relay - Persistent Interface ID option DHCPv6 Relay Agent notification for Prefix Delegation
- PIM SSM Mapping
- VRF lite NSF support with routing protocols OSPF/EIGRP/BGP

- Supported MIBs
 - Cisco Enhanced Image MIB
 - Cisco HSRP extension MIB
 - CISCO-CALLHOME-MIB.my
 - EnergyWise MIB
 - POE MIB
 - POE ext MIB
 - Entity-Diag-MIB
 - Bridge MIB
- Time Protocols (SNTP, TimeP) master

On Supervisor Engine 6L-E

- Community PVLAN support
- Ethertype Classification
- QinQ
- PPPoE IA (or Intermediate Agent)

New Hardware Features in Release 12.2(52)SG

Release 12.2(52)SG provides the following new hardware for the Catalyst 4500 series switch:

- PWR-C45-6000ACV, Catalyst 4500 series switch 6000 Watt AC power supply'

New Software Features in Release 12.2(52)SG

Release 12.2(52)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

All Supervisor Engines

- EnergyWise
- Switch and IP Phone interaction for security features
 - Port Security
 - DHCP Snooping
 - Dynamic ARP Inspection
 - BPDU Guard
- Network Mobility Services Protocol
- Identity ACL Policy Enforcement Enhancement
 - Filter-ID
 - Per-user ACL
- Smart Call Home*
- Management Port Features with IPv6

- Local WebAuth Enhancement
- MDA with Voice Assignment
- HSRP v2 for IPv4
- HSRP v2 or IPv6
- DHCPv6 Enhancements
 - DHCPv6 Ethernet Remote ID option
 - DHCPv6 Relay - Persistent Interface ID option DHCPv6 Relay Agent notification for Prefix Delegation
- SSM Mapping
- PIM Accept Register - Rogue Multicast Server Protection (**route-map** option is not supported)
- VRF lite NSF support with routing protocols OSPF/EIGRP/BGP
- Supported MIBs
 - Cisco Enhanced Image MIB
 - Cisco HSRP extension MIB
 - CISCO-CALLHOME-MIB.my
 - EnergyWise MIB
 - POE MIB
 - POE ext MIB
 - Entity-Diag-MIB
 - Bridge MIB

On Supervisor Engine 6-E

- Community PVLAN support
- Ethertype Classification
- PBR
- QinQ
- PPPoE IA (or Intermediate Agent)

New Hardware Features in Release 12.2(50)SG3

Release 12.2(50)SG3 provides the following hardware for the Catalyst 4500 series switch:

- CVR-X2-SFP10G
Hot-swappable input/output (I/O) converter module that fits into a 10-Gigabit Ethernet X2 slot on a switch or line card module. Hosts one 10-Gigabit Ethernet SFP+ transceiver module.
- SFP-10G-SR, Cisco 10GBASE-SR SFP+ Module for MMF

New Software Features in Release 12.2(50)SG3

Release 12.2(50)SG3 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(50)SG2

Release 12.2(50)SG2 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(50)SG2

Release 12.2(50)SG2 provides no new features for the Catalyst 4500 series switch.

New Hardware Features in Release 12.2(50)SG1

Release 12.2(50)SG1 provides no new hardware for the Catalyst 4500 series switch.

New Software Features in Release 12.2(50)SG1

Release 12.2(50)SG1 provides the following Cisco IOS software features for the Catalyst 4500 series switch:

- EEM version 2

For information on EEM, see the URL:

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

New Hardware Features in Release 12.2(50)SG



Note

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(50)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis.

Release 12.2(50)SG provides the following new hardware for the Catalyst 4500 series switch:

- X2-10GB-ZR optical module
- X2-10GB-DWDM optical module
- Classic Series 48-port 10/100/1000 Premium PoE line card

New Software Features in Release 12.2(50)SG

Release 12.2(50)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:



Note

The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

**Note**

The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

- IGMP Querier (“Configuring IGMP Snooping” chapter)
- OSPF and EIGRP fast convergence and protection (Refer to the Cisco IOS Release 12.4 documentation)
- CDP 2nd Port Status TLV (no configuration required on the switch)

**Note**

The link up/down information in the CDP Second Port Status TLV (added by the Cisco IP Phones Host Movement Detection enhancement) allows the switch to de-authenticate devices which were previously authenticated. The phone must have firmware release 8.1(1) or later to generate this CDP TLV.

- ANCP Client (not supported on E-Series Supervisor Engine 6-E; “Configuring ANCP Client” chapter)
- **boot config** command (Refer to the Cisco IOS Release 12.2 documentation)
- Archiving Crashinfo Files (“Configuring Command-Line Interfaces” chapter)
- Boot Configuration/Crash Dump (refer to the Cisco IOS Release 12.2 documentation)
- Downloadable ACLs (“Configuring Network Security with ACLs” chapter)
- Ethernet Management Port (Refer to the “Configuring Interfaces” chapter)
- Flexible Authentication Sequencing (“Configuring 802.1X” chapter)
- Inactivity Timer (“Configuring 802.1X” chapter)
- Multi-Authentication (“Configuring 802.1X” chapter)
- Open Authentication (“Configuring 802.1X” chapter)
- PPPoE Intermediate Agent (not supported on E-Series Supervisor Engine 6-E; “PPPoE Circuit-Id Tag Processing” chapter)
- VRF-aware IP services (“Configuring VRF-Lite” chapter)
- VTP version 3 (“Configuring VLANs, VTP, and VMPS” chapter)
- Web Authentication (“Configuring Web Authentication” chapter)
- Configuration Rollback
- Cisco TrustSec SGT Exchange Protocol (SXP) IPv4

For more information, refer to the following URLs:

<http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html>

On Supervisor Engine 6-E

- Bidirectional PIM (“Configuring IP Multicast” chapter)
- Control Plane Policing (“Configuring CPP” chapter)
- DHCP Relay Agent for IPv6 (refer to Cisco IOS Release 12.2 mainline documentation)
- Multicast VRF-lite (“Configuring VRF-Lite” chapter)
- On Board Failure Logging (refer to the Cisco IOS Release 12.2 documentation)

- Private VLAN trunks (“Configuring Private VLANs” chapter)
- SVI Auto State Exclude (“Configuring Layer 3 Interfaces” chapter)
- Unicast MAC filtering (“Configuring Network Security with ACLs” chapter)
- QoS for IPv6 (refer to the Cisco IOS Release 12.4T documentation)

New Hardware Features in Release 12.2(46)SG



Note

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(46)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis.

Release 12.2(46)SG provides the following new hardware for the Catalyst 4500 series switch:

- 20 W PoE linecard

New Software Features in Release 12.2(46)SG

Release 12.2(46)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:



Note

The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

On Supervisor Engine 6-E

- 802.1X Enhancements (Refer to the “Configuring 802.1X” chapter)
 - 802.1X Guest VLAN
 - 802.1X Critical Authentication
 - Wake on LAN
 - Radius Accounting
 - Radius Supplied Timeout
- ARP QoS (Refer to the “Configuring QoS” chapter)
- Per-VLAN CTI (Refer to the “Configuring QoS” chapter)
- Catalyst 4900M switch support for Layer 3 features
- RSPAN (Refer to the “Configuring SPAN and RSPAN” chapter)

On all the Supervisor Engines (II-Plus thru 6-E)

- FlexLink and FlexLink+ with MAC Address-Table Move Update (Refer to the “Configuring FlexLink” chapter)
- LLDP-MED: location TLV and MIB (Refer to the “Configuring LLDP and LLDP-MED” chapter)
- Auto-MDIX Disable (Refer to the “Configuring Interfaces” chapter)
- Enhanced Object Tracking (EOT) (Refer to the Cisco IOS Release 12.2 documentation)

- HSRP with EOT
- VRRP with EOT
- GLBP with EOT
- IP SLA with EOT
- Reliable Backup Static Routing with EOT
- CFM 802.1ag (Refer to the “Configuring Ethernet CFM and OAM” chapter)
- E-OAM 802.3ah (Refer to the “Configuring Ethernet CFM and OAM” chapter)

**Note**

The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

New Hardware Features in Release 12.2(44)SG

**Note**

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(44)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis.

Release 12.2(44)SG provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4624-SFP-E

New Software Features in Release 12.2(44)SG

Release 12.2(44)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

**Note**

The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

On Supervisor Engine 6-E

- High availability on Supervisor Engine 6-E (SSO/NSF) (Refer to the “Configuring NSF on SSO” chapter)
- High availability on Supervisor Engine 6-E (ISSU) (Refer to the “Configuring ISSU” chapter)
- Embedded management (Refer to the Cisco IOS Release 12.4 documentation)
- MAC notify MIB (Refer to the Cisco IOS Release 12.4 documentation)
- IPv4_BGP, IPv6_BGP (Refer to the Cisco IOS Release 12.4 documentation)
- 802.1X Dynamic VLAN Assignment (Refer to the “Configuring 802.1X” chapter)
- 802.1X MAC Authentication Bypass (Refer to the “Configuring 802.1X” chapter)
- 802.1X with VVID/PVID (Refer to the “Configuring 802.1X” chapter)

- High availability, 2+2 10GE or 4+4 1GE active uplinks (Refer to the “Configuring Interfaces” chapter)
- Enhanced Power over Ethernet Support ((Refer to the “Configuring Power over Ethernet” chapter)
- Eight configurable queues per port (Refer to the “Configuring QoS” chapter)

On all the Supervisor Engines (II-Plus thru 6-E)

- EEM with ISSU

For details, refer to the EEM Home Page:

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

- ESM

For details, refer to the ESM Home Page:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_esm.html

- VSS client with PagP+

After configuring VSS dual-active on a Catalyst 6500 switches, the Catalyst 4500 series switch can detect VSS dual-active with PagP+ support.

- IP SLA (Refer to the Cisco IOS Release 12.2 documentation)
- 802.1ab LLDP and 802.1ab LLDP-MED (Refer to the “Configuring LLDP and LLDP-MED” chapter)
- X2 Link Debounce Timer (Refer to the “Configuring Interfaces” chapter)
- Resilient Ethernet Protocol (REP) (Refer to the “Configuring REP” chapter)



Note

The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

New Hardware Features in Release 12.2(40)SG



Note

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(40)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis.

A brief list of primary E-Series hardware supported by Cisco IOS Release 12.2(40)SG includes the following:

- WS-C4503-E - Cisco Catalyst 4500 E-Series 3-Slot Chassis, fan, no power supply
- WS-C4506-E - Cisco Catalyst 4500 E-Series 6-Slot Chassis, fan, no power supply
- WS-C4507R-E - Cisco Catalyst 4500 E-Series 7-Slot Chassis, fan, no power supply, redundant supervisor capability
- WS-C4510R-E - Cisco Catalyst 4500 E-Series 10-Slot Chassis, fan, no power supply, redundant supervisor capability
- WS-X45-Sup6-E - Cisco Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ TwinGig
- WS-X4648-RJ45V-E - Cisco Catalyst 4500 E-Series 48-Port PoE 802.3af 10/100/1000(RJ45)

- WS-X4648-RJ45V+E - Cisco Catalyst 4500 E-Series 48-Port Premium PoE 10/100/1000
- WS-X4606-X2-E - Cisco Catalyst 4500 E-Series 6-Port 10GbE (X2)

New Software Features in Release 12.2(40)SG

Release 12.2(40)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:



Note

The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Only available on Supervisor Engine 6-E

- Dynamic Multi-Protocol Ternary Content Addressable Memory (Configuring Network Security with ACLs” chapter)
- Service-Aware Resource Allocation (Refer to the Cisco IOS Release 12.4 documentation)
- Unicast Reverse Path Forwarding (“Configuring Unicast Reverse Path Forwarding” chapter)
- IPv6 Forwarding in Hardware (Refer to the Cisco IOS Release 12.4 documentation)
- Enhanced Interior Gateway Routing Protocol IPv6 Support (Refer to the Cisco IOS Release 12.4 documentation)
- IPv6 Multicast Listener Discovery Snooping (“Configuring MLD Snooping” chapter)
- TwinGig Converter Module (“Configuring Interfaces” chapter)
- Robust and Flexible File Management System (FAT File System) (Refer to the Cisco IOS Release 12.4 documentation)
- Storm Control: Per-Port Multicast Suppression (“Configuring Storm Control” chapter)
- Cisco Modular QoS Command-Line Interface (“Configuring QoS” chapter)
- Two-Rate Three-Color Policing

Only available on Supervisor Engines II-Plus thru V-10GE

- Selecting Mode of Capturing Control Packets (Configuring Network Security with ACLs” chapter)
- Layer 2 Control Policing (“Configuring QoS” chapter)

Available on all Supervisor Engines (II-Plus thru 6-E)

- Gateway Load Balancing Protocol (Refer to the Cisco IOS Release 12.4 documentation)
- Option 82 Enhancement (“Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts” chapter)



Note

The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

Upgrading the System Software

In most cases, upgrading the switch to a newer release of Cisco IOS software does not require a ROMMON upgrade. However, if you are running an early release of Cisco IOS software and plan to upgrade, refer to the following tables for the minimum Cisco IOS image and the recommended ROMMON release, respectively.


Note

You must upgrade to ROMMON Release 12.2(44r)SG5 to run Cisco IOS Release 12.2(54)SG on the Supervisor Engine 6-E and Supervisor Engine 6L-E.


Caution

Most supervisor engines have the required ROMMON release. However, due to caveat CSCed25996, we recommend that you upgrade your ROMMON to the recommended release.

Table 8 Supervisor Engine and Minimum Cisco IOS Release

Supervisor Engine	Minimum Cisco IOS Release
IV	12.1(12c)EW or 12.1(14)E
II-Plus	12.1(19)EW
II-Plus-10GE	12.2(25)SG
V	12.2(18)EW
II-Plus-TS	12.2(20)EWA
V-10GE	12.2(25)EW
ME-X4924-10GE	12.2(31)SGA
6-E	12.2(40)SG
6L-E	12.2(52)XO

Table 9 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Minimum ROMMON Release	Recommended ROMMON Release
IV	12.1(12r)EW	12.2(31r)SGA1
II-Plus	12.1(19r)EW	12.2(31r)SGA1
II-Plus-10GE	12.2(25r)SG	12.2(31r)SGA3
V	12.1(20r)EW1	12.2(31r)SGA1
II-Plus-TS	12.2(20r)EW	12.2(31r)SGA1
V-10GE	12.2(25r)EW	12.2(31r)SGA3
ME-X4924-10GE	12.2(25r)EW	12.2(31r)SGA1
6-E	12.2(44r)SG5	12.2(44r)SG5
6L-E	12.2(44r)SG5	12.2(44r)SG5

Table 10 **ROMMON Release and Promupgrade Programs**

ROMMON Release	Promupgrade Program
12.1(11br)EW	cat4000-sup3-promupgrade-121_11br_EW
12.1(12r)EW	cat4000-sup3-promupgrade-121_12r_ew
12.1(19r)EW	cat4000-ios-promupgrade-121_19r_EW
12.1(20r)EW1	cat4000-ios-promupgrade-121_20r_EW1
12.1(20r)EW2	cat4000-ios-promupgrade-121_20r_EW2
12.2(20r)EW	cat4000-ios-promupgrade-122_20r_EW
12.2(20r)EW1	cat4000-ios-promupgrade-122_20r_EW1
12.2(31r)SG3	cat4500-ios-promupgrade-122_31r_SG3
12.2(31r)SGA1	cat4500-ios-promupgrade-122_31r_SGA1
12.2(31r)SGA	cat4500-e-ios-promupgrade-122_31r_SGA3
12.2(40r)SG	cat4500-e-ios-promupgrade-122_40r_SG
12.2(44r)SG1	cat4500-e-ios-promupgrade-122_44r_SG1
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5

The following sections describe how to upgrade your switch software:

- [Identifying an +E Chassis and ROMMON, page 45](#)
- [Guidelines for Upgrading the ROMMON, page 46](#)
- [Upgrading the Supervisor Engine ROMMON from the Console, page 46](#)
- [Upgrading the Supervisor Engine ROMMON Remotely Using Telnet, page 49](#)
- [Upgrading the Cisco IOS Software, page 53](#)

Identifying an +E Chassis and ROMMON

An +E chassis is identified by a FRU minor value in the chassis' idprom.

When supervisor engine 1 (sup1) is in ROMMON and supervisor engine 2 (sup2) is in IOS, only sup2 can read the idprom contents of chassis' idprom. Chassis type is displayed as "+E" in the output of the **show version** command. Conversely, sup1 can only display the chassis type as "E."

When both sup1 and sup2 are in ROMMON, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

When both sup1 and sup2 are in IOS, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

Guidelines for Upgrading the ROMMON


Caution

If your supervisor engine is shipped with a newer version of ROMMON then do not downgrade! The new ROMMON will have board settings based on a hardware revision of components, and old settings will not work.

Upgrading the Supervisor Engine ROMMON from the Console


Caution

To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.


Note

The examples in this section use the programmable read-only memory (PROM) upgrade version 12.1(20r)EW1 and Cisco IOS Release 12.1(20)EW1. For other releases, replace the ROMMON release and Cisco IOS software release with the appropriate releases and filenames.

Follow this procedure to upgrade your supervisor engine ROMMON:

Step 1

Directly connect a serial cable to the console port of the supervisor engine.


Note

This section assumes that the console baud rate is set to 9600 (default). If you want to use a different baud rate, change the configuration register value for your switch.

Step 2

Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch that is upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4000 system images.

Step 3

Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, replace **bootflash:** with **slot0:**.

Step 4

Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
[OK - 455620 bytes]
```

Step 5

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#

Enter the **reload** command to reset the switch, press **Ctrl-C** to stop the boot process, and re-enter ROMMON.

The following example shows the output after a reset into ROMMON:

```
Switch# reload
Proceed with reload? [confirm]

03:57:16:%SYS-5-RELOAD:Reload requested

*****
*
* Welcome to Rom Monitor for WS-X4515 System.
* Copyright (c) 2002 by Cisco Systems, Inc.
* All rights reserved.
*
*****

Rom Monitor Program Version 12.1(12r)EW

.
.(output truncated)
.

Established physical link 100MB Half Duplex
Network layer connectivity may take a few seconds
rommon 1 >
```

Step 6

Run the PROM upgrade program by entering this command:
boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

**Caution**

No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the output from a successful upgrade, followed by a system reset:

```
rommon 2 > boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

*****
*
* Rom Monitor Upgrade Utility For WS-X4515 System
* This upgrades flash Rom Monitor image to the latest
*
* Copyright (c) 2002, 2003 by Cisco Systems, Inc.
* All rights reserved.
*
*****

Image size = 314.236 KBytes

Maximum allowed size = 511.75 KBytes

Upgrading your PROM... DO NOT RESET the system
unless instructed or upgrade of PROM will fail !!!
```

```
Beginning erase of 0x80000 bytes at offset 0x3f80000... Done!

Beginning write of prom (0x4e8ec bytes at offset 0x3f80000)...

This could take as little as 30 seconds or up to 2 minutes.
Please DO NOT RESET!

Success! The prom has been upgraded successfully.
System will reset itself and reboot in about 15
```

Step 7 Boot the Cisco IOS software image, and enter the **show version** command to verify that ROMMON has been upgraded to 12.1(20r)EW1.

Step 8 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the **cat4000-ios-promupgrade-121_20r_EW1** image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:
```

```
All deleted files will be removed, proceed (y/n) [n]? y
```

```
Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L3 Switch Software (cat4500-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC
```

ROM: 12.1(20r)EW1

Dagobah Revision 86, Swamp Revision 28

```
Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-i9s-mz.121-20.EW1"
```

```
cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.
```

```
Configuration register is 0x2102
```

```
Switch#
```

The ROMMON has now been upgraded.

See the [“Upgrading the Cisco IOS Software”](#) section on page 53 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet



Caution

To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow this procedure to upgrade your supervisor engine ROMMON to Release 12.1(20r)EW1. This procedure can be used when console access is not available and when the ROMMON upgrade must be performed remotely.



Note

In the following section, use the PROM upgrade version cat4000-ios-promupgrade-121_20r_EW1.

Step 1

Establish a Telnet session to the supervisor engine.



Note

In the following discussion, we assume that at least one IP address has been assigned to either an SVI or a routed port.

Step 2

Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4500 system images.

Step 3

Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, replace **bootflash:** with **slot0:**.

Step 4

Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

Step 5

Use the **no boot system flash bootflash:file_name** command to clear all BOOT variable commands in the configuration file. In this example, the BOOT variable was set to boot the image cat4000-i5s-mz.121-19.EW1.bin from bootflash:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-i5s-mz.121-19.EW1.bin
Switch(config)# exit
```

```
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Use the `boot system flash bootflash:file_name` command to set the BOOT variable. You will use two BOOT commands: one to upgrade the ROMMON and a second to load the Cisco IOS software image after the ROMMON upgrade is complete. Notice the order of the BOOT variables in the example below. At bootup the first BOOT variable command upgrades the ROMMON. When the upgrade is complete the supervisor engine will autoboot, and the second BOOT variable command will load the Cisco IOS software image specified by the second BOOT command.



Note The `config-register` must be set to autoboot.

In this example, we assume that the console port baud rate is set to 9600 bps and that the `config-register` is set to 0x0102.

Use the `config-register` command to autoboot using image(s) specified by the BOOT variable. Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version 12.1(20r)EW1. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco IOS software Release 12.1(20)EW1.

config-register to 0x0102.

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# boot system flash bootflash:cat4000-i9s-mz.121-20.EW1
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

- Step 6** Use the `show bootvar` command to verify the boot string. The BOOT variable in this example will first run the PROM upgrade to upgrade ROMMON. Then, the upgrade software will reload and the supervisor engine will load the Cisco IOS software image.

```
Switch# sh bootvar
BOOT variable = bootflash:cat4000-ios-promupgrade-121_20r_EW1,1;bootflash:cat400
0-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

- Step 7** Run the PROM upgrade program by issuing the `reload` command. Issuing this command will terminate your Telnet session.



Caution

Verify the boot string in step 6. No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the console port output from a successful ROMMON upgrade followed by a system reset. Your Telnet session is disconnected during the ROMMON upgrade, so you will not see this output. This step could take 2-3 minutes to complete. You will need to reconnect your Telnet session after 2-3 minutes when the Cisco IOS software image and the interfaces are loaded.

```
Switch#reload
Proceed with reload? [confirm]

1d05h: %SYS-5-RELOAD: Reload requested

*****
*
* Welcome to Rom Monitor for WS-X4515 System.
* Copyright (c) 2002 by Cisco Systems, Inc.
* All rights reserved.
*
*****

Rom Monitor Program Version 12.1(12r)EW

Board type 2, Board revision 7
Swamp FPGA revision 28, Dagobah FPGA revision 86

***** The system will autoboot in 5 seconds *****

Type control-C to prevent autobooting.
. . . . .
Established physical link 100MB Full Duplex
Network layer connectivity may take a few seconds

***** The system will autoboot now *****

config-register = 0x0102
Autobooting using BOOT variable specified file.....

Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1

*****
*
* Rom Monitor Upgrade Utility For WS-X4515 System
* This upgrades flash Rom Monitor image to the latest
*
* Copyright (c) 2002, 2003 by Cisco Systems, Inc.
* All rights reserved.
*
*****

Image size = 314.236 KBytes

Maximum allowed size = 511.75 KBytes

Upgrading your PROM... DO NOT RESET the system
unless instructed or upgrade of PROM will fail !!!
```

```
Beginning erase of 0x80000 bytes at offset 0x3f80000... Done!

Beginning write of prom (0x4e8ec bytes at offset 0x3f80000)...

This could take as little as 30 seconds or up to 2 minutes.
Please DO NOT RESET!

Success! The prom has been upgraded successfully.
System will reset itself and reboot in about 15
.
.(output truncated)
.
***** The system will autoboot now *****
```

```
config-register = 0x0102
Autobooting using BOOT variable specified file.....

Current BOOT file is --- bootflash:cat4000-i9s-mz.121-20.EW1

Rommon reg: 0x56000380

Running IOS...
```

```
Decompressing the image
#####
#####
#####
#####
#####
##### [OK]
```

- Step 8** Use the **no boot system flash bootflash:file_name** command to clear the BOOT command used to upgrade the ROMMON.

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

- Step 9** Use the **show version** command to verify that the ROMMON has been upgraded.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC
```

```
ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28
```

```
Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4000-i9s-mz.121-20.EW1"
```

```
cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
```

```

3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

```

Configuration register is 0x0102

Switch#

- Step 10** Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the cat4000-ios-promupgrade-121_20r_EW1 image from bootflash and reclaim unused space:

```

Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

```

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y

Switch#

- Step 11** Use the **show bootvar** command to verify that the ROMMON upgrade program has been removed from the BOOT variable.

```

Switch#sh bootvar
BOOT variable = bootflash:cat4000-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0102

```

The ROMMON has now been upgraded.

See the [“Upgrading the Cisco IOS Software” section on page 53](#) for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software



Caution

To avoid actions that might make your system unable to boot, please read this entire section before starting the upgrade.

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved
Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.
- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.

- To upgrade the Cisco IOS software on your Catalyst 4500 series switch, use this procedure:

Step 1

Step 2

Step 3

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-is-mz.121-8a.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

- Step 5** Use the **boot system flash** command to add the Cisco IOS software image to the BOOT variable. The following example shows how to add the cat4000-is-mz.121-12c.EW image to the BOOT variable:

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-12c.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

- Step 6** Use the **config-register** command to set the configuration register to 0x2102. The following example show how to set the second least significant bit in the configuration register:

```
Switch# configure terminal
Switch(config)# config-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

- Step 7** Enter the **reload** command to reset the switch and load the software.



Caution

No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process by performing a reset, power cycle, or OIR of the supervisor, for at least five minutes.

The following example shows the output from a successful upgrade followed by a system reset:

```
Switch# reload
Rommon reg: 0x2B004180

Upgrading FPGA...

Decompressing the image
##### [OK]

*****
*
* WS-X4014 FPGA Upgrade Utility For WS-X4014 Machines *
*
* Copyright (c) 2002 by Cisco Systems, Inc.
* All rights reserved.
*
*****

Image size = 483.944 KBytes

Maximum allowed size = 1023.75 KBytes

Upgrading your FPGA image... DO NOT RESET the system
unless instructed or upgrade of FPGA will fail !!!

Beginning erase of 0x100000 bytes at offset 0x3d00000... Done!

Beginning write of fpga image (0x78fb0 bytes at offset 0x3d00000)...
```

This could take as little as 30 seconds or up to 2 minutes.
Please DO NOT RESET!

Success! FPGA image has been upgraded successfully.
System will reset itself and reboot in about 15 seconds.
0

```
*****
*
* Welcome to Rom Monitor for WS-X4014 System.
* Copyright (c) 2002 by Cisco Systems, Inc.
* All rights reserved.
*
*****
```

Rom Monitor Program Version 12.1(12r)EW

Board type 1, Board revision 5
Swamp FPGA revision 16, Dagobah FPGA revision 47

```
MAC Address   : 00-30-85-XX-XX-XX
IP Address    : 10.10.10.91
Netmask       : 255.255.255.0
Gateway       : 10.10.10.1
TftpServer    : Not set.
Main Memory   : 256 MBytes
```

**** The system will autoboot in 5 seconds ****

Type control-C to prevent autobooting.
Switch#

Step 8 Use the **show version** command to verify that the new Cisco IOS release is operating on the switch.

Limitations and Restrictions

These sections list the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4500 series switch.

All Supervisor Engines

- When you enter the **permit any any ?** command you will observe the **octal** option, which is unsupported in Cisco IOS Release 12.2(54)SG.
CSCsy31324
- A Span destination of fal is not supported.
- The "keepalive" CLI is not supported in interface mode on the switch, although it will appear in the running configuration. This behaviour has no impact on functionality.

- TDR is only supported on interfaces Gi1/1 through Gi1/48, at 1000BaseT under open or shorted cable conditions. TDR length resolution is +/- 10 m. If the cable is less than 10 m or if the cable is properly terminated, the TDR result displays "0" m. If the interface speed is not 1000BaseT, an "unsupported" result status displays. TDR results will be unreliable for cables extended with the use of jack panels or patch panels.
- The following guidelines apply to Fast UDLD:
 - Fast UDLD is disabled by default.
 - Configure fast UDLD only on point-to-point links between network devices that support fast UDLD.
 - You can configure fast UDLD in either normal or aggressive mode.
 - Do not enter the link debounce command on fast UDLD ports.
 - Configure fast UDLD on at least two links between each connected network device. This reduces the likelihood of fast UDLD incorrectly error disabling a link due to false positives.
 - Fast UDLD does not report a unidirectional link if the same error occurs simultaneously on more than one link to the same neighbor device.
- A XML-PI specification file entry does not return the desired CLI output.

The outputs of certain commands, such as **show ip route** and **show access-lists**, contain non-deterministic text. While the output is easily understood, the output text does not contain strings that are consistently output. A general purpose specification file entry is unable to parse all possible output.

Workaround (1):

While a general purpose specification file entry may not be possible, a specification file entry might be created that returns the desired text by searching for text that is guaranteed to be in the output. If a string is guaranteed to be in the output, it can be used for parsing.

For example, the output of the `show ip access-lists SecWiz_Gi3_17_out_ip` command is this:

```
Extended IP access list SecWiz_Gi3_17_out_ip
 10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
 20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
 30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

The first line is easily parsed because access list is guaranteed to be in the output:

```
<Property name="access list" alias="Name" distance="1.0" length="-1" type="String"
/>
```

The remaining lines all contain the term host. As a result, the specification file may report the desired values by specifying that string. For example, this line

```
<Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

will produce the following for the first and second rules

```
<rule>
  deny
</rule>
```

and the following for the third statement

```
<rule>
  permit
</rule>
```

Workaround (2):

Request the output of the **show running-config** command using NETCONF and parse that output for the desired strings. This is useful when the desired lines contain nothing in common. For example, the rules in this access list do not contain a common string and the order (three permits, then a deny, then another permit), prevent the spec file entry from using permit as a search string, as in the following example:

```
Extended MAC access list MACCOY
  permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
  permit any host 65de.edfe.fefe xns-idp
  permit any any protocol-family rarp-non-ipv4
  deny host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
  permit any any
```

The XML output of **show running-config** command includes the following, which can then be parsed programmatically, as desired:

```
<mac><access-list><extended><ACLName>MACCOY</ACLName></extended></access-list></mac>
  <X-Interface> permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000
  appletalk</X-Interface>
  <X-Interface> permit any host 65de.edfe.fefe xns-idp</X-Interface>
  <X-Interface> permit any any protocol-family rarp-non-ipv4</X-Interface>
  <X-Interface> deny host 005e.1e5d.9f7d host 3399.e3e1.ff2c
  dec-spanning</X-Interface>
  <X-Interface> permit any any</X-Interface>
```

- Although the Catalyst 4500 series switch still supports legacy 802.1X commands used in Cisco IOS Release 12.2(46)SG and earlier releases (that is, they are accepted on the CLI), they do not display in the CLI help menu.
- Current IOS software cannot support filenames exceeding 64 characters.
- All software releases support a maximum of 32,768 IGMP snooping group entries.
- For any configuration where the source-interface keyword is used, if you provide an SVI that is associated with a secondary private VLAN, configuration involving the secondary VLAN may be lost when the switch is reloaded. In such scenarios, always use the primary private VLAN.

For Supervisor Engines II+Plus through V-10GE

- For the IP Unnumbered feature, the following are not supported:
 - Dynamic routing protocols
 - HSRP/VRRP
 - Static ARP
 - Unnumbered interface and numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
 - GRE encapsulation forwarding method
 - Hash bucket based assignment method
 - Redirection on an egress interface (redirection out)
 - Redirect-list ACL
- For IPX software routing, the following are not supported:

- NHRP (Next Hop Resolution Protocol)
 - NLSP
 - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
 - AURP
 - AppleTalk Control Protocol for PPP
 - Jumbo Frames
 - EIGRP
- For the NetFlow feature, the following limitations apply:
 - NetFlow will not account for control packets, packets that encountered link-level errors, and ARP/RARP packets.
 - The software cache for NetFlow is fixed, users cannot change the size.
 - The statistical distribution row that displays the distribution across various packet sizes is not available.
- For the PBR feature, the following limitations apply:
 - Packet length-based matching policies are not supported.
 - IP Precedence, TOS and Qos groups are fixed.
 - ACL/Route-map statistics are not updated.
- IGRP is not supported (use EIGRP instead).
- The MAC address table is cleared when you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- While running NSF and IS-IS IETF mode, if you enter the **issu runversion** command within 5 minutes of entering the **issu loadversion** command, packet loss may occur during an ISSU upgrade.
Workaround: Configure the NSF interval timer to 0 minutes, or delay entering the **issu runversion** command until the NSF interval timer expires and NSF restarts.
- Routes may not be properly redistributed from one routing protocol to another when NSF is enabled on the switch. The success of the redistribution depends on the order in which the routing protocols converge after an NSF switchover.
Workaround: None.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect because only classless routing is supported. The **ip classless** command is not supported because classless routing is enabled by default.
- The Catalyst 4510R switch does not support Supervisor Engines II-Plus, III, IV, and II-Plus-10GE. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or Supervisor Engine IV in a prior release.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.

- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the [“Troubleshooting” section on page 426](#) for alternatives.
- You cannot downgrade to Cisco IOS Release 12.1(8a)EW1 after running Release 12.1(13)EW (or higher). If you need to downgrade, contact your TAC representative for further instructions, and mention caveat CSCdz59058.
- Observe the following standard Cisco IOS software behavior when deploying redundant supervisor engines in a Catalyst 4507R chassis: While the startup configuration file is being parsed, the configuration file is not applied to hardware that does not exist.

For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

This situation does not occur when both supervisor engines are present in the chassis.

Workaround: Copy the startup configuration file into the running configuration:

```
Switch# copy startup-config running-config
```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not damage your system, you might want to remove it to avoid confusion.

Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of the **show standby GigabitEthernet1/1** command output:

```
switch(config)# interface g1/1
switch(config)# no standby 0 name (0 is hsrp group number)
```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, which ensures that a hello is received before HSRP leaves the initiate state.

Use the **standby delay reload** option if the router is rebooting after reloading the image.

- When you attempt to run OSPF between a Cisco router and a third-party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

Workaround: Because the problem is caused by mismatched MTUs, you should change the MTU on either router to match the other's MTU.

- You can run .1q-in-.1q packet passthrough with a Supervisor Engine III and a Supervisor Engine IV, but you can run only .1q-in-.1q encapsulation with a Supervisor Engine II+10GE, Supervisor Engine V, and Supervisor Engine V-10GE.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW supports a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Only ports 1 and 2 on the WS-X4418-GB module and ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- If an original packet is dropped due to transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.

- For all software releases, do not use over 100,000 routes.
- Use the **no ip unreachable** command on all interfaces with ACLs configured for performance reasons.
- Layer 3 path load-balancing metrics are not supported in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, 12.1(19)EW, and 12.1(20)EW. (CSCdv10578)
- The threshold for the Dynamic ARP Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- A limited number of ACL bindings are dynamically installed by the IP source guard feature on a Catalyst 4500 series switch Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use Supervisor Engine IV.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- By default, IPv6 is not enabled. To route IPv6, you must enter the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (after IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- When you use private VLANs on the WS-4516 module, old ARP entries will not time out of the ARP cache if you do not manually clear the entry. This event has no effect on production.
- Compact flash formatted in Cisco IOS Release 12.2(20)EW should be reformatted in Release 12.2(25)EW on both Supervisor Engine V-10GE and non-Supervisor V-10GE systems. Compact flash formatted on any other release does not need to be reformatted on non-Supervisor Engine V-10GE systems.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting up. Doing so may cause a failure in the online diagnostics test.
Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)
- When used in conjunction with a 10-slot chassis, Supervisor Engine V only supports the Catalyst 4500 series two-port Gigabit Ethernet line card (WS-X4302-GB) in the 10th slot.
- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.
- Support for PoE depends on the use of line cards and power supplies that support PoE.

PoE switching modules:

- WS-X4148-RJ45V
- WS-X4224-RJ45V
- WS-X4248-RJ45V

- WS-X4248-RJ21V
- WS-X4524-GB-RJ45V
- WS-X4548-GB-RJ45V
- 'WS-X4548-GB-RJ45V+

PoE-enabled power supplies:

- PWR-C45-1300ACV
 - PWR-C45-1400DC
 - PWR-C4K-2800AC
 - PWR-C45-1400AC
 - PWR-C45-1300ACV
 - 'PWR-C45-6000ACV'
- The maximum number of mappings for configuring PVLAN promiscuous trunk ports is 500 primary VLANs to 500 secondary VLANs.
 - The 802.1X inaccessible authentication bypass feature is not supported with the NAC LAN port IP feature.
 - Changes to the console speed in line console 0 configuration mode do not affect console speed in ROMMON. To apply the same console speed in ROMMON, use the confreg ROMMON utility.
 - Supervisor Engine II-Plus does not support compact flashes formatted by an Cisco IOS image prior to Cisco IOS Release 12.2(19)EW.
 - If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to following appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not responding.
```

If this message appears, verify that the switch is connected to the ACS. You should also ensure that the switch has been properly configured as an AAA client on the ACS.

- The **bgp shutdown** command is not supported in BGP router configuration mode. Entering this command might produce unexpected results.
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

Workaround: Disable idle timeouts. (CSCec30214)

- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat appears in all software releases.

Workarounds:

1. Disable inline power on the switch ports using the **power inline never** command.
 2. Configure the media converter to autonegotiate the speed and duplex instead of running them at 100 Mbps and full duplex. (CSCee62109)
- IPSG for static hosts supports the same port mode as IPSG except that it does not support trunk port:
 - It supports Layer 2 access port and PVLAN host port (isolated or community port).
 - It does not support trunk port, Layer 3 port, or EtherChannel.

- IPSG for static hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches CoS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.
- If a set of DSCP values are already configured (for example, 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbi dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. You must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbi dscp-based 8-63** command will leave 0-7 selected.
- When you use Port Security with Multi Domain Authentication (MDA) on an interface:
 - Allow for at least three MAC addresses to access the switch: two for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
 - Ensure that the data and voice VLAN IDs differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
 - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. CPU usage will drop after the hosts are learned.
 - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.
 - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as Inactive.
 - Autostate SVI does not work on EtherChannel.
- With the resolution of CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area. However, a system-defined GARP class in Control Plane Policing (CPP) still exists.
- Certain configurations on the Catalyst 4507R and Catalyst 4510R chassis exceed the available maximum data power. These configurations include a combination of the follow PIDs:
 - Seven-slot configuration
 - Chassis WS-C4507R-E, WS-C4510R-E
 - Dual supervisor WS-X45-Sup6-E
 - One or more of the models WS-X4448-GB-RJ45 or WS-X4148-FX-MT

To maximize the 10/100/1000 port density of 7- and 10-slot chassis when using redundant Supervisor Engine 6-E, install WS-X4548-GB-RJ45 instead of WS-X4448-GB-RJ45 line cards. If you require WS-X4448-GB-RJ45 line cards, two options are available:

- Option 1
Only four line card slots can be used on the Catalyst 4507R and six line card slots on the Catalyst 4510R chassis.
- Option 2
When all slots are required, only one model WS-X4448-GB-RJ45 line card can be used.

To maximize the 100-BASE-FX port density of 7 and 10 slot chassis when using Supervisor Engine 6-E install WS-4248-FE-SFP line cards with FX optics instead of WS-X4148-FX-MT line cards. If WS-X4148-FX-MT line cards are required, two options are available:

- Option 1

You can use only 4 linecard slots on the Cat4507R chassis and 6 line card slots on the Cat4510R chassis.

- Option 2

When all slots are required, you can only use one WS-X4448-GB-RJ45 line card.

- When IPv6 is enabled on an interface through any CLI, you might see the following message:

```
% Hardware MTU table exhausted
```

In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This will happen if no room exists in the hardware MTU table to store additional values.

To create room in the table, unconfigure some unused MTU values. Then, either disable or reenable IPv6 on the interface, or reapply the MTU configuration.

- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

To enable IPSG with static hosts on a port, enter the following commands:

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
```



Caution

If you configure the **ip verify source tracking [port-security]** interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.



Note

The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- You must disable hardware control plane policing by removing the **system-cpp-policy** named ACL from the controlplane before performing an ISSU upgrade between Cisco IOS Release 12.2(40)SG and a previous release. You cannot detach **system-cpp-policy** named ACL from the controlplane in previous releases. If you are running a previous release, you must first upgrade to the latest maintenance release in the Cisco IOS Release 12.2(31) SGAx while performing an ISSU upgrade to Cisco IOS Release 12.2(40)SG.
- On a Supervisor Engine V-10GE (WS-X4516-10GE), if a startup configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not start with the new uplink mode. After you copy the startup configuration with the new uplink mode into flash memory, you must change the uplink mode to the new uplink mode through the command interface before the system is power cycled. This ensures that the system starts in the new uplink mode.
- When you use Supervisor Engine V in a Catalyst 4510R or 4510R-E chassis, slot 10 (FlexSlot) only supports the following linecards: the two-port GBIC (WS-X4302-GB) and the Access Gateway Module (WS-X4604-GWY). Supervisor Engine V-10GE has this same restriction when you

configure its uplink select mode to **all**. Supervisor Engine V-10GE supports all Catalyst 4500 Series linecards in slot 10 when its uplink select mode is configured as **tengigabitethernet** or **gigabitethernet**. Supervisor Engine 6-E supports all Catalyst 4500 series linecards in slot 10.

- Prior to Cisco IOS Release 12.2(50)SG, on switches with Supervisor Engines V, V-10GE and earlier, class-map hit statistics on a user defined class-map in system-cpp-policy are not updated properly. With Cisco IOS Release 12.2(50)SG, the hit statistics for user-defined class-map in the system-cpp-policy are updated properly. However, in per-vlan capture mode, the hit stats for system defined in system-cpp-policy are not updated. In the global capture mode, hit stats for all class-maps (user-defined and system-defined) in the system-cpp-policy are updated properly.
- If you use MDA or multi-auth host mode in conjunction with pre-authentication open access, a switch ignores unicast EAPOL responses.

Workarounds:

- Force the supplicant to use multicast EAPOL.
- Avoid authentication open mode

CSCtq33048

For Supervisor Engine 6-E and Supervisor Engine 6L-E

- The Catalyst 4510R switch does not support Supervisor Engines 6L-E. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- The MAC address table is cleared while you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, because only classless routing is supported. The command **ip classless** is not supported because classless routing is enabled by default.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the [“Troubleshooting” section on page 426](#) for alternatives.
- When you deploy redundant supervisors in a Catalyst 4507R, for hardware that does not exist while the startup configuration file is being parsed, the configuration file for the hardware is not applied. For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

This situation will not occur when both supervisor engines are physically in the chassis.

Workaround: Copy the startup configuration file into the running configuration:

```
Switch# copy startup-config running-config
```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not harm your system, you might want to remove it to avoid confusion.

Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of **show standby GigabitEthernet1/1** command output:

```
switch(config)# interface g1/1
switch(config)# no standby 0 name (0 is hsrp group number)
```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, thereby ensuring that a hello is received before HSRP leaves the initiate state.

Use the **standby delay reload** option if the router is rebooting after reloading the image.

- When you attempt to run OSPF between a Cisco router and a third party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

Workaround: Ensure that the MTUs match.

- You can run only .1q-in-.1q packet pass-through with Supervisor Engine 6-E.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW support a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Because the Supervisor Engine 6-E supports the FAT filesystem, the following restrictions apply:

- The **verify** and **squeeze** commands are not supported.
- The **rename** command is supported in FAT file system.

For Supervisor Engine 6-E, the **rename** command is available for bootflash and slot0. For all other supervisor engines, the **rename** command is supported for nvram devices only.

- The **fsck** command is supported for slot0 device. It is not supported in the file systems on supervisor engines other than 6-E.
- In the FAT file system, the IOS **format bootflash:** command erases user files only. It does not erase system configuration.
- The FAT file system supports a maximum of 63 characters for file/directory name. The maximum for path length is 127 characters.
- The FAT file system does not support the following characters in file/directory names: { } # % ^ and space characters.
- The FAT file system honors the Microsoft Windows file attribute of read-only and read-write, but it does not support the Windows file hidden attribute.
- Supervisor Engine 6-E uses the FAT file system for compact flash (slot0). If a compact flash is not formatted in FAT file system (such as compact flash on a supervisor engine other than 6-E), the switch does not recognize it.
- If an original packet is dropped because of transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- All software releases support a maximum of 16,000 IGMP snooping group entries.
- To maximize performance, use the **no ip unreachable** command on all interfaces that are configured for ACLs.
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.

- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting. Doing so may cause the online diagnostics test to fail.

Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)

- The **switchport private-vlan mapping trunk** command supports a maximum of 500 unique private VLAN pairs. For example, 500 secondary VLANs could map to one primary VLAN, or 500 secondary VLANs could map to 500 primary VLANs.
- Support for PoE depends on the use of the following line cards and power supplies.

PoE switching modules:

- WS-X4148-RJ45V
- WS-X4224-RJ45V
- WS-X4248-RJ45V
- WS-X4248-RJ21V
- WS-X4524-GB-RJ45V
- WS-X4548-GB-RJ45V
- WS-X4648-RJ45V-E
- WS-X4648-RJ45V+E
- WS-X4548-GB-RJ45V+

PoE enabled power supplies:

- PWR-C45-1300ACV
- PWR-C45-1400DC
- PWR-C4K-2800AC
- PWR-C45-1400AC
- PWR-C45-1300ACV
- PWR-C45-6000ACV

- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not responding.
```

If this message appears, ensure network connectivity exists between the switch and the ACS. Also check that the switch has been properly configured as an AAA client on the ACS.

- For IP Port Security (IPSG) for static hosts, the following apply:
 - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. The CPU usage will drop after the hosts are learned.
 - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.

- Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as inactive.
- Autostate SVI does not work on EtherChannel.
- When IPv6 is enabled on an interface with any CLI, you might see the following message:

```
% Hardware MTU table exhausted
```

In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This occurs if no room exists in the hardware MTU table to store additional values.

To create room, unconfigure some unused MTU values. Then, either disable or re-enable IPv6 on the interface, or reapply the MTU configuration.

- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

To enable IPSG with static hosts on a port, enter the following commands:

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
```



Caution

If you configure the **ip verify source tracking [port-security]** interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.



Note

The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- uRPF supports up to four paths. If a packet arrives at one of the valid VLANs that is not programmed as one of the RPF VLAN in hardware, it is dropped. If traffic may arrive from any other interfaces without RPF configured, it can be switched.
- Input and output ACLs cannot override or filter traffic received on an uRPF interface.
- No CLI command exists to reflect uRPF drop packets during hardware switching. The **sh ip traffic** and **show cef int** commands do not reflect uRPF drops.
- IPv6 ACL is not supported on a switchport. IPv6 packets cannot be filtered on switchports using any of the known methods: PACL, VACL, or MACLS.
- Class-map match statements using **match ip prec | dscp** match only IPv4 packets, whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match CoS in the same class-map with the IPv6 access-list has any mask within the range /81 and /127. This situation causes forwarding packets to software, which efficiently disables the QoS.
- When the following data-only Catalyst 4500 linecards are used in a Catalyst 4507R-E or 4510R-E chassis with Supervisor Engine 6-Es, the capacity of the power supply may be exceeded:
 - WS-X4148-FX-MT Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX (MT-RJ)
 - WS-X4448-GB-RJ45 Cisco Catalyst 4500 48-port 10/100/1000 Module (RJ-45)

The Catalyst 4503-E and Catalyst 4506-E have no caveats. The Catalyst 4507R-E configurations that use power supplies rated at 1400 W or above also have no caveats.

The following replacement switching modules will not exceed the power supply capacity for any Catalyst 4500-E chassis:

	Recommended Replacement	Description
WS-X4148-FX-MT	WS-X4248-FE-SFP	Fast Ethernet, 48-port 100BASE-X (SFP)
WS-X4448-GB-RJ45	WS-X4548-GB-RJ45	Enhanced 48-port 10/100/1000 Module (RJ-45)
WS-X4448-GB-RJ45	WS-X4648-RJ45V-E	E-Series 48-port 802.3af PoE 10/100/1000 (RJ-45)

Refer to the *Catalyst 4500 Series Module Installation Guide* to determine the power requirements for all of the Catalyst 4500 linecards and the power capacities of the Catalyst 4500 power supplies.

- Supervisor Engine 6-E *only* supports Catalyst 4500 Series linecards in slots 8-10.
- If you remove a line card from a redundant switch and initiate an SSO switch-over, then reinsert the line card, all interfaces are shutdown. The remaining configuration on the original line card is preserved.

This situation only occurs if a switch reached SSO before you removed the line card.

- On Supervisor Engine 6-E, upstream ports support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- Supervisor Engine 6-E supports fast UDLD on a maximum of 32 ports.
- With Cisco IOS Release 12.2(53)SG3 (and 12.2(54)SG), we changed the default behavior such that your single supervisor, RPR, or fixed configuration switch does not reload automatically. To configure automatic reload, you must enter the **diagnostic fpga soft-error recover aggressive** command. (CSCth16953)

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.



Note

All caveats in Release 12.4 also apply to the corresponding 12.1 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL:

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124MCAVS.html



Note

For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL:

<http://tools.cisco.com/security/center/publicationListing.x>

Open Caveats for Cisco IOS Release 12.2(54)SG1

This section lists the open caveats for Cisco IOS Release 12.2(54)SG1:

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
Police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.
(CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet

	QueueID	Old QueueName	New QueueName
	8	<unused queue>	control-packet
	11	<unused queue>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the **no switchport** command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. (CSCta61825)

Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Despite the different default value, you can configure any value in the time range.

Workaround: None. CSCte51948

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

CSCsv69853

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

CSCsv90044

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- If you disable and re-enable IGMP Snooping on a VLAN, the output of the **show mac address** command does not display the [term] Switch against the multicast entry. Multicast traffic is not impacted.

Workaround: Do **shut**, then **no shut** on the SVI. CSCtg72559

- When a connected data device behind a phone disconnects from a port configured for multi-auth host mode, a new session for the device is restarted even though the device is absent.

The CDP TLV generated to indicate that a data device has disconnected is ignored. This is done to avoid disconnecting other connected data clients, if any. (Refer to CSCta47293.)

Workarounds: Enter either of the following commands:

- **clear authentication session interface**
- **authentication timer inactivity**

CSCtg83631

- If an X2 or SFP is in an inactive uplink port on a Supervisor Engine V-10GE, Supervisor II+10GE, Supervisor 6-E, or Supervisor 6-LE, it may cause threshold violations to be reported once every 10 minutes.

Workaround: Remove the X2 or SFP from the port. CSCth08212

- When Fallback WebAuth and Multi-host are configured on a port and no PACL exists, **permit ip any any** is installed in the TCAM and all traffic from the host is allowed to pass.

Workaround: Configure an ACL on the port. CSCte18760

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- If host-mode multi-domain is configured and authorization succeeds, traffic may not pass from an IP phone or a data device.

Workaround: None. CSCtj56811

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.
(CSCtn68186)

- When a switch is configured for MAC Authentication Bypass (MAB) EAP and the AAA server requests EAP-TLS (as the EAP method) first, MAB fails.

Workarounds:

- Configure the switch port for *mab* rather than *mab eap*.
- Configure the AAA server to propose EAP-MD5 first rather than EAP-TLS for MAB EAP requests. CSCti78674

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None.

If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- When CX1 or SFP+ is plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None. CSCtc46340

- Before large PACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec 1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pac1 - now
fully loaded in hardware *Dec 1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

Workaround: No functional impact.

You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- RA Guard counters are not incremented in the output of the **show ipv6 first-hop counters interface** command when Router Advertisement and Router Redirect packets with Destination address FF02::x are dropped.

Workaround: None. CSCtf69108

- ND/NS packets are dropped when an IPv6 ACL is attached to an Layer 3 interface.

Workaround: Add the following permit ACEs to the ACL:

```
permit icmp any any nd-ns
permit icmp any any nd-na
```

CSCtg77035

- A switch crashes when attaching a service-policy to a target, provided the service-policy contains more than 56 classes each with an explicit marking action, such as :

```
policy-map pm
class c0
  set dscp default
  set cos 0
class c1
  set dscp 1
  set cos 1
class c2
  set dscp 2
  set cos 2
... ..
class c56
  set dscp cs7
  set cos 0
```

Workaround: Use tablemap-based marking. CSC99836

Resolved Caveats in Cisco IOS Release 12.2(54)SG1

This section lists the resolved caveats in Release 12.2(54)SG1:

- Catalyst 4500 series switches may lose the per-vlan maximum mac addresses for port-security when the link goes down. This applies to the following interface configuration :

```
switchport port-security maximum <number> vlan access
switchport port-security maximum <number> vlan voice
```

Workaround: None. CSCti74791

- If **no vtp** is configured on ports that receive VTP updates, a switch no longer processes Layer 2 control traffic (STP and CDP).

Workaround: Upgrade to 12.2(53)SG3, 12.2(50)SG8, or later. CSCth00398

- In a redundant chassis with numerous PoE linecards (WS-X4548-GB-RJ45V, WS-X4548-RJ45V+), undergoing a switchover, the CPU utilization exceeds 80 percent on the new active supervisor engine.



Note In a non-redundant chassis with the same PoE linecards , CPU utilization will not reach 80 percent.

This issue is not applicable to fixed config chassis.

Workaround: None. CSCti08570

- A Supervisor Engine 6-E or Supervisor Engine 6L-E running cat4500e-ipbasek9-mz.122-53.SG1 might experience a reload because of interface flapping.

Workaround: None. CSCtf49878

- When software reads the hardware status of a linecard before it fully initializes, a supervisor engine experiences a software-initiated crash.

Workaround: None. CSCtf82009

- The Spanning Tree process disables VLAN on a trunk interface if it was configured for VLAN Mapping Translation.

Workaround: Configure **spanning-tree bpdudfilter enable** in configuration interface mode.

CSCtj21636

- When at least one 1:1 translation is configured, same to same VLAN mapping is disallowed. This impacts customers who want to switch packets on certain VLANs without VLAN Translation.

Workaround: None

CSCti22918

- Pinging to SVI fails when VLAN mapping is configured (1 to 1 same VLAN and different VLAN mapping).

If you randomly add or remove VLANs in a VLAN database, SVI traffic stops on some VLANs.

Workaround: None. CSCtk03191

- When the **show ip ospf int** command is paused while the backup designated router neighbor goes down, a switch may reload when you enter the **show ip ospf int** command:

```
c3560sw2# show ip ospf int
Vlan804 is up, line protocol is up
  Internet Address 10.0.0.2/24, Area 0
  Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.2, Interface address 10.0.0.2
  --More--
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
  changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan804, changed
  state to down
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Vlan804 from FULL to DOWN,
  Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
```

The next line in the output of the **show ip ospf int** command is the following:

```
Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1
```

If you now advance the output by pressing either **Enter** or the space bar, the device reloads and the following error message displays:

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```

Workaround: None. CSCtd73256

- The **show tacacs+** command does not provide private tacacs+ server statistics.

Workaround: None. CSCta96363

- A switch can crash with a Watchdog NMI Vector 000 and CRC error as follows:

```
"%C4K_SUPERVISOR-2-FPGASOFTERROR: Memory inconsistency detected" have
```

appeared on the switch followed by link flaps, transceiver (HAMM module, X2, sfp) insertion/removal on uplinks (base board ports on 4900M)

Workarounds:

- Reload the switch when the error message displays.
- Upgrade to Cisco Catalyst Release 12.2(54)SG1, Cisco Catalyst Release 12.2(53)SG4 (and later), when available.

CSCtk75675

Open Caveats for Cisco IOS Release 12.2(54)SG

This section lists the open caveats for Cisco IOS Release 12.2(54)SG:

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<unused queue>	control-packet
	11	<unused queue>	adj-same-if
	13	acl input log	rpf-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct. CSCsz20149

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the **no switchport** command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command. CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. (CSCta61825)

Workaround: None CSCtb30327

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Despite the different default value, you can configure any value in the time range.

Workaround: None. CSCte51948

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

CSCsv69853

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

CSCsv90044

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- If you disable and re-enable IGMP Snooping on a VLAN, the output of the **show mac address** command does not display the [term] Switch against the multicast entry. Multicast traffic is not impacted.

Workaround: Do **shut**, then **no shut** on the SVI. CSCtg72559

- When a connected data device behind a phone disconnects from a port configured for multi-auth host mode, a new session for the device is restarted even though the device is absent.

The CDP TLV generated to indicate that a data device has disconnected is ignored. This is done to avoid disconnecting other connected data clients, if any. (Refer to CSCta47293.)

Workarounds: Enter either of the following commands:

- **clear authentication session interface**
- **authentication timer inactivity**

CSCtg83631

- If an X2 or SFP is in an inactive uplink port on a Supervisor Engine V-10GE, Supervisor II+10GE, Supervisor 6-E, or Supervisor 6-LE, it may cause threshold violations to be reported once every 10 minutes.

Workaround: Remove the X2 or SFP from the port. CSCth08212

- When Fallback WebAuth and Multi-host are configured on a port and no PACL exists, **permit ip any any** is installed in the TCAM and all traffic from the host is allowed to pass.

Workaround: Configure an ACL on the port. CSCte18760

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- If host-mode multi-domain is configured and authorization succeeds, traffic may not pass from an IP phone or a data device.

Workaround: None. CSCtj56811

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.

(CSCtn68186)

- When a switch is configured for MAC Authentication Bypass (MAB) EAP and the AAA server requests EAP-TLS (as the EAP method) first, MAB fails.

Workarounds:

- Configure the switch port for *mab* rather than *mab eap*.
- Configure the AAA server to propose EAP-MD5 first rather than EAP-TLS for MAB EAP requests. CSCti78674

Supervisor Engine 6-E and Supervisor Engine 6L-E Specific Caveats

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None.

If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then later allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- When CX1 or SFP+ is plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None. CSCtc46340

- Before large ACLs are fully loaded in hardware, you might observe a false completion messages like the following:

```
Dec 1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec 1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

Workaround: No functional impact.

You must wait for the ACLs to be programmed before performing other TCAM related changes. CSCtd57063

- RA Guard counters are not incremented in the output of the **show ipv6 first-hop counters interface** command when Router Advertisement and Router Redirect packets with Destination address FF02::x are dropped.

Workaround: None. CSCtf69108

- ND/NS packets are dropped when an IPv6 ACL is attached to an Layer 3 interface.

Workaround: Add the following permit ACEs to the ACL:

```
permit icmp any any nd-ns
permit icmp any any nd-na
```

CSCtg77035

- A switch crashes when attaching a service-policy to a target, provided the service-policy contains more than 56 classes each with an explicit marking action, such as :

```
policy-map pm
class c0
    set dscp default
    set cos 0
class c1
    set dscp 1
    set cos 1
class c2
    set dscp 2
    set cos 2
...
class c56
    set dscp cs7
    set cos 0
```

Workaround: Use tablemap-based marking. CSC99836

Resolved Caveats in Cisco IOS Release 12.2(54)SG

This section lists the resolved caveats in Release 12.2(54)SG:

- When you configure **switchport block multicast** on a switch running Cisco IOS Release 12.2(53)SG1 or 12.2(50)SG6, Layer 2 multicast is not blocked.

Prior to Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, the **switchport block multicast** command would block IP Multicast, Layer 2 multicast, and broadcast traffic .

Workaround: None. CSCta61825

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be forwarding.

Workaround: Enter **shut**, then **no shut** on the port. CSCta04665

- When you request an on demand Call Home message send without specifying a profile name and the specified module returns an unknown diagnostic result, the following error message displays:

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules. CSCsz05888

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you forward traffic from a traffic generator at a high rate, a security violation is wrongly flagged.

Workaround: None. CSCsy38640

- On a switch running Cisco IOS Release 12.2(54)SG, when the access VLAN is deleted and then restored on a port configured with 802.1X multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a disabled state after the access VLAN is restored.

Workaround: Shut down then reopen the interface. CSCso50921

- When you configure **ip source binding** statically on an interface, and then remove the linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a linecard, delete the statically configured **ip source binding** entries on any of the interfaces on the line-card. (CSCsv54529)

- Performing a default interface operation on an interface with auto-QoS enabled results in an error message and the loss of the auto-QoS configuration. For example, the following sequence of operation results in a loss of the configuration:

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

Workaround: Replace the **default interface** command with the following:

```
config# interface interface-number
config-if# switchport
```

(CSCsq47116)

- Initially, REP configured with VLAN Load Balancing (VLB) works correctly. When you issue a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut**, then **no-shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

Workaround: Unconfigure any generic QoS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family. (CSCsq84796)

- IPv6 MLD entries are active even if an IPv6 MLD related configuration does not exist.

Workaround: Unconfigure all generic QoS policies from the system. CSCsq84853

- You observe a .05% loss on WS-X4908-10GE when sending traffic at 99% of the port capacity.

Workaround: None. CSCsl39767

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Detach and re-attach the service-policy, provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map).

If this occurs on the default queue, modify and reset some queuing parameters like bandwidth or shape. CSCsk62457

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. CSCsk67395)

- A switch fails if you configure a PBR policy to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map to only match on ACL(s). CSCtg22126

For the SFP+ optical modules SFP-10G-LRM, SFP-10G-LR, and SFP-10G-SRA, a Tx low power alarm displays when either IOS boots or you replace the module. This is an initial false alarm upon detection of a new SFP+ module; subsequently, it clears.

SFP and 10GBASE-CU SFP+ modules do not show this problem.

Workaround: None. CSCtg82213

- If a third-party non-PoE device is connected to a WS-4648-RJ45V-E or WS-4648-RJ45V+E and PoE is enabled, when the device reboots, the link does not come up. An error message might display on the device.

Workaround: Disable PoE (through entering the **power inline never** command in interface configuration mode).

In Cisco IOS Release 12.2(54)SG, you can enter the **power inline autoneg-advertise** command in global config mode to enable linkup. CSCtb78851

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a port is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None. CSCsx64308

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None. CSCsu35604

- A switch crashes if a PBR policy, configured to match on prefix-list(s) instead of ACL(s), is attached to an interface.

This happens provided one the following conditions apply:

- A route map matching on prefix-list is attached to an input interface as a PBR policy.
- A route map for PBR (already attached to an interface) is configured or modified to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map for PBR to only match on ACLs.

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may ported out another interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file with a maximum of 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts causes convergence timing to exceed 300ms.

Workaround: None. CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This impacts restoration timing but not REP functionality. After a REP segment fails, traffic restoration time sometimes exceeds 200ms.

CSCsx55704

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, you must remove the engines completely before re-insertion.

CSCsy70428

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. CSCsv43819

- The IP router option may not work with IGMP version 2.

Workaround: None. CSCsv42869

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: Enter the **queue-limit** command to specify an explicit queue size. CSCso06422

- After three failed authentication attempts, WinXP stops responding to EAPOL requests from the switch that caused the 802.1X timeout (default or configured). After the timeout, WinXP moves to auth-fail VLAN.

Workaround: Attempt an authorization after a timeout. CSCte84432

- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode is configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) is configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- When you load an unsupported Catalyst 4500 software version on WS-C4507R+E and WS-C4510R+E, the following log messages are seen and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type"
```

Or

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type"
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type 14" (where n is a slot number)
```

Workaround: Load Cisco IOS Release 12.2(54)SG or 12.2(53)SG4 on WS-C4507R+E and WS-C4510R+E. CSCtl70275

Open Caveats for Cisco IOS Release 12.2(53)SG9

This section lists the open caveats for Cisco IOS Release 12.2(53)SG9:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are incremented correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a port is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: Add entries to the Default ACL in addition to 'deny ip any any'.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R+E and WS-C4510R+E and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or
```

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later.

CSCtl70275

- If a port is configured for Private VLAN and is authorized in a guest VLAN, a traceback appears on the console.

Workaround: None.

CSCtq73579

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
```

```
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.
- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **`no switchport trunk native vlan tag`** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where *n* is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCtl84092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-C4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCtl89329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCtl74638

Resolved Caveats in Cisco IOS Release 12.2(53)SG9

This section lists the resolved caveats in Release 12.2(53)SG9:

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

- The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat>

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

CSCtg47129

Open Caveats for Cisco IOS Release 12.2(53)SG8

This section lists the open caveats for Cisco IOS Release 12.2(53)SG8:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<unused queue>	control-packet

QueueID	Old QueueName	New QueueName
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running
Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: Add entries to the Default ACL in addition to 'deny ip any any'.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R+E and WS-C4510R+E and none of the ports come up:

%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or

%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and

%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type 14" (where n is a slot number)

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later. CSCtl70275

- If a port is configured for Private VLAN and is authorized in a guest VLAN, a traceback appears on the console.

Workaround: None. CSCtq73579

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.
- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure vlan dot1q tag native globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where n is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCtl84092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCtl89329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCtl74638

Resolved Caveats in Cisco IOS Release 12.2(53)SG8

This section lists the resolved caveats in Release 12.2(53)SG8:

- While processing a CDP frame, a switch may crash after displaying SYS-2-FREEFREE and SYS-6-MTRACE messages.

Workaround: Enter the **no cdp run** command to disable CDP. CSCub45763

Open Caveats for Cisco IOS Release 12.2(53)SG7

This section lists the open caveats for Cisco IOS Release 12.2(53)SG7:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```

000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby

```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```

Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes

```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<unused queue>	control-packet
	11	<unused queue>	adj-same-if
	13	acl input log	rpf-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.
Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693)
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3  
context:145 length:11) due to: invalid context
```


Workaround: None. This is an informational message. (CSCsi60898)
- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.
Workaround: None. (CSCsm30320)
- An IP unnumbered configuration is lost after a switch reloads.
Workarounds: Do one of the following:
 - After a reload, copy the startup-config to the running-config.
 - Use a loopback interface as the target of the **ip unnumbered** command.
 - Change the CLI configuration so that during bootup the router port is created first.
 (CSCsq63051)
- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```


Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)
- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.
Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)
- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.
Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)
- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.
Workaround: Shut down, and then reopen the interface. (CSCso50921)
- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.
Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)
- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running
Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: Add entries to the Default ACL in addition to 'deny ip any any'.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R+E and WS-C4510R+E and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or
```

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later.

CSCtl70275

- If a port is configured for Private VLAN and is authorized in a guest VLAN, a traceback appears on the console.

Workaround: None. CSCtq73579

- While processing a CDP frame, a switch may crash after displaying SYS-2-FREEFREE and SYS-6-MTRACE messages.

Workaround: Enter the **no cdp run** command to disable CDP. CSCub45763

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.

CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.

- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **`no switchport trunk native vlan tag`** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where *n* is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCtl84092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCtl89329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCtl74638

Resolved Caveats in Cisco IOS Release 12.2(53)SG7

This section lists the resolved caveats in Release 12.2(53)SG7:

- If you use AAA accounting with the **`broadcast`** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **`broadcast`** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>



Note

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:
authentication event server dead action authorize...
authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

Open Caveats for Cisco IOS Release 12.2(53)SG6

This section lists the open caveats for Cisco IOS Release 12.2(53)SG6:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: cl (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

	QueueID	Old QueueName	New QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<unused queue>	control-packet
	11	<unused queue>	adj-same-if
	13	acl input log	rpf-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.

- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: Add entries to the Default ACL in addition to 'deny ip any any'.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R+E and WS-C4510R+E and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or
```

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later.

CSCtl70275

- If a port is configured for Private VLAN and is authorized in a guest VLAN, a traceback appears on the console.

Workaround: None.

CSCtq73579

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>



Note

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:
authentication event server dead action authorize...
authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.
- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where *n* is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCtl84092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-C4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCtl89329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCtl74638

Resolved Caveats in Cisco IOS Release 12.2(53)SG6

This section lists the resolved caveats in Release 12.2(53)SG6:

- A switch ignores unicast EAPOL responses, when you use MDA or multi-auth host mode combination with authentication open.

Workarounds:

- Force the supplicant to use multicast EAPOL.
- Avoid authentication open mode. CSCtq33048

- When you enter the **rep preempt segment** command, the MAC might not flush.

Workaround: Re-enter the **rep preempt segment** command.

CSCtr89862

- A switch crashes following changes to policy-based routing (route-map).

Workaround: Ensure that a policy is configured on an interface prior to changing a default next-hop in route-map. CSCtr31759

- The following problems are experienced with IPv6 SNMP, when an IPv4 address is not configured:
 - Traps are not sent through IPv6.
 - SNMP GETs sent to a switch IPv6 address trigger a traceback.

Workaround: Perform the following task:

1. Disable the SNMP engine with the **no snmp-server** command.
2. Configure an IPv4 address and an IPv6 address on loopback interfaces.
3. Enable the SNMP engine.

CSCsw76894

- If you enable SNMP before assigning an IPv4 address, SNMP does not listen for requests.

Workaround: Perform the following task:

1. Disable the SNMP engine with the **no snmp-server** command.

2. Configure an IP address and an IPv6 address on loopback interfaces.
3. Enable the SNMP engine.

CSCsw92921

- When flex link load balancing is used, MAC addresses sourced over the backup interface are not programmed into the dynamic MAC address table. Source address learning is triggered for all traffic from these MAC addresses, which may cause high CPU.

Workaround: Configure static MAC addresses for the source addresses on the backup flex link interface. CSCtr40070

- On networks with round-trip-time (RTT) delay of 5 milisec and over, IP SLA ethernet jitter probes are stuck in NoConnection/Busy/Timeout state:

```
uPE1#sh ip sla stat | inc Timeout
Latest RTT: NoConnection/Busy/Timeout
```

Issue is likely not to appear in environments with low latency (<5msec).

Workarounds:

- None (regarding ethernet jitter probe)
 - Consider using the IP sla ethernet echo probes to collect RTT statistics. CSCtb96522
 - A system may crash if it receives more than 10 MA (Management Address) TLVs per LLDP neighbor entry.
- Workaround:** Disable LLDP MA TLV sending on the peers. CSCtj22354
- Querying rttMonHistory objects using an invalid index causes a switch to crash.
- Workaround:** Use **getnext** rather than **get** to list valid indicies for the MIB OID. CSCtr52740
- Registering a TCL policy may cause the switch to hang.
- Workaround:** None. CSCto72927
- Flooded multicast traffic is not sent over a port channel interface after a member link or port-channel flaps.

Workarounds:

- Delete and add impacted VLAN with **no vlan** *vlan_id* and **vlan** *vlan_id* commands.
- Flap the impacted port channel with the **shutdown** and **no shutdown** commands. CSCtr17251
- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

Open Caveats for Cisco IOS Release 12.2(53)SG5

This section lists the open caveats for Cisco IOS Release 12.2(53)SG5:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .IX with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.

- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: Add entries to the Default ACL in addition to 'deny ip any any'.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R+E and WS-C4510R+E and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or
```

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later.

CSCtl70275

- If a port is configured for Private VLAN and is authorized in a guest VLAN, a traceback appears on the console.

Workaround: None.

CSCtq73579

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

**Note**

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:

authentication event server dead action authorize...

authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.
- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure vlan dot1q tag native globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where *n* is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCt184092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCt189329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCt174638

Resolved Caveats in Cisco IOS Release 12.2(53)SG5

This section lists the resolved caveats in Release 12.2(53)SG5:

- When you specify a proxy ACL ACE with an extra space, the proxy ACL is not programmed for authenticated and authorized hosts.

Workarounds:

- Do not provide an extra space while specifying a proxy ACL ACE.
- Use a Downloadable ACL or a Filter-ID ACL rather than a proxy ACL. CSCtk67010

- When the egress policy-map is applied to an “single” active port, you cannot modify the multicast control packets (HSRP and OSPF) IP ToS field.

Workaround: None. CSCtg60011

- Interfaces connected to a Catalyst 4500 series switch remain linked up though no active supervisor engines exist.

This occurs when a peer switch is connected to a line card in a non-redundant switch and you reload the active supervisor engine. Some interfaces on some linecards remain linked up. Far-end switches must rely on protocol timeouts to detect the switch’s reload.

This situation only occurs with the WS-X4648-RJ45-E and WS-X4548-RJ45-V-E line cards.

Workaround: Reset the linecards with the **hw module module n** command, then reload the switch. CSCt11764

- Some non-powered devices fail to linkup when connected to a 4648-RJ45-E/+E line card port with a 2 or 4-wire cable (1,2,3,6).

Workarounds:

- Use a 4-pair wire.
- Enter the **power inline never** command.
- Enter the **speed auto 10 100** command. CSCtn43537

- When reconnecting to a switch using IP device tracking, a Windows Vista, Windows 2008, or Windows 2007 device registers a duplicate address message.

Workaround: Disable gratuitous ARP on the Windows device. CSCtn27420

- 802.1X supplicants connected to ports in a guest VLAN fail the initial authentication.

Workarounds:

- Configure the supplicant to retry 802.1X.
- Connect or disconnect to the port. CSCtl89361

- The switch crashes when AAA accounting packets are generated for web authentications.

Workaround: Disable AAA accounting. CSCtl77241

- When IP SLA probes are configured and active for a period of 72 weeks, and you poll the rttmon mib for probe statistics, the router reloads.

The problem is not observed for another 72 weeks.

Workaround: None. CSCsl70722

- If a device is connected to multiple ports on the switch and **no ip routing** is configured, ARP entries display in an incorrect VLAN (**pv vlan** appears in the entry).

Workaround: Configure **ip routing**. CSCtj20399

- When a switch is using 802.X with web authentication, and you open an http session, you see a login screen using http, rather than https.

This happens only if you use a custom banner configured like the following:

```
ip auth-proxy auth-proxy-banner http ^C Custom Banner here ^C
```

Workaround: Remove the custom banner. CSCtb77378

- If you change the authentication method for a client to webauth before removing the fallback configuration, web authentication is triggered.

Workarounds:

- Reconfigure 802.1X with the **no dot1x pae authenticator/dot1x pae authenticator** command.
- Reload the switch. CSCtd43793

- LLDP packets are sent (.1q) tagged when the native VLAN of the of the dot1q trunk is not the default (VLAN 1).

LLDP IEEE standard requires frames sent untagged. With this issue, some peer devices may reject the tagged LLDP frame.

Workaround: Use the default native VLAN for the trunks. CSCtn29321

- When a redundant power supply is turned off, ciscoEnvMonAlarmContacts returns 00 even though the LED on the supervisor engine is orange.

Workaround: If you include **snmp-server enable traps envmon** in the device configuration, a `ciscoEnvMonSuppStatusChangeNotification` is generated when the power supply either turns off or fails. CSCtl72109

- A switch might crash if **ip cef accounting non-recursive** is configured and BGP routes are being supplied.

Workaround: Disable IP cef accounting. CSCtn68186

- A port channel will not establish correctly if the following conditions apply:
 - **vlan dot1q tag native** is configured.
 - Either the native VLAN is not allowed on the trunk, or the peer does not accept tagged channel protocol packets.

Workaround: None. CSCtj90471

- A power supply can be listed as removed, but continues to function normally. This behavior is illustrated by the following system messages:

```
%C4K_IOSMODPORTMAN-4-POWERSUPPLYREMOVED: Power supply 1 has been removed
%C4K_CHASSIS-3-INSUFFICIENTPOWERSUPPLIESDETECTED: Insufficient power supplies present
for specified configuration
%C4K_CHASSIS-2-INSUFFICIENTPOWERDETECTED: Insufficient power available for the
```

Workaround: None. CSCtn38000

- High CPU results from constant MAC learning when multiple REP rings are used, each with a different VLAN list.

Workaround: Ensure that all trunk ports in the REP ring topology have the same list of VLANs, including ports in other REP rings that export STCNs into the REP ring where the problem is observed. CSCto67625

- DHCP clients renewing through a load-balanced DHCP relay on an unnumbered interface may be unable to renew their lease because the renew ACK is lost.

Workaround: Avoid using DHCP load balancing. CSCth00482

- If a switch is configured for multiple authentication host-mode, and an interface on that switch is configured for 802.1X, that interface disallows unidirectional port control, breaking the functionality of Wake on LAN.

Workaround: Use a different host-mode. CSCti92970

- A memory leak caused by corrupted SSH packets is detected in SSH process during internal testing.

Workaround: Allow SSH connections only from trusted hosts. CSCth87458

- If you provide extra space anywhere in between while specifying a proxy ACL ACE, the proxy ACL is not programmed for authenticated and authorized hosts.

Workarounds

- Do not provide any extra space while specifying a proxy ACL ACE.
- Use DACL or Filter-Id ACL instead of proxy ACLs. CSCtk67010
- In multi-auth mode, when you disconnect a PC behind a Cisco IP phone, the data session is not removed.

This behavior is anticipated. In multi-auth mode, the system cannot distinguish between the data client that is attached to the phone and those that are attached to the switch through a hub.

Workaround: None. CSCtd70009

- A switch crashes when you use **no set extcommunity cost** to remove **set extcommunity cost** in a route-map and you enter **show run**.

Workaround: Remove the entire route-map and re-create it. CSCsr23563

- On a SSH and telnet-configured switch, if you configure a banner, then SSH to the router, the banner shows incorrectly:

```
pqiu@apt-cse-613% ssh cisco@10.66.79.211
"$(hostname) via line $(line) $(line-desc)"
```

Here is how you configured the banner:

```
banner login ^CC
$(hostname) via line $(line) $(line-desc)
^C
!
```

If you telnet to the router, the banner shows correctly as follows:

```
"SV-9-5 via line 67"
```

Workaround: None. CSCei24145

- After you boot a reloaded switch in a REP ring topology, the soon-to-be alternate port forwards traffic and causes a loop. This continues until you enter **shut** and **no shut** on the alternate port.

Workaround: Enter **shut** and **no shut** on the alternate interface. CSCtn03533

- If a static route is configured for an RP address that is reachable from a directly connected network, the switch does not send a PIM register toward the RP.

Workaround: Avoid configuring overlapping IP addresses. CSCtj96095

Open Caveats for Cisco IOS Release 12.2(53)SG4

This section lists the open caveats for Cisco IOS Release 12.2(53)SG4:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if

	QueueID	Old QueueName	New QueueName
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- A switch might fail an ftp to a dhcp-snooping file if the file's size is 0 Kb.

Workaround: When creating the file, enter some characters, remove the **ftp** command, then re-enter it as follows:

```
Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
```

CSCsk38763

- The following messages are displayed when you load an supported version of Catalyst 4500 software on WS-C4507R-E and WS-C4510R-E and none of the ports come up:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
or
```

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
and
```

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

Workaround: Load Cisco IOS Releases 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later.

CSCtl70275

- A proxy ACL is not programmed for authenticated and authorized hosts, when you specify a proxy ACL ACE with an extra space

Workarounds:

- Do not provide an extra space while specifying a proxy ACL ACE.
- Use a Downloadable ACL or a Filter-ID ACL instead of a proxy ACL.

CSCtk670101

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.

(CSCtn68186)

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCTr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

**Note**

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:
authentication event server dead action authorize...
authentication event server alive action reinitialize
- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

When Supervisor Engine II+10GE attempts to boot in a non-production 4510R+E chassis, the following error message is displayed:

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10 09 08 07 06 05 04 03 02 01 "
```

Supervisor Engine II+10GE is not supported on a ten-slot chassis. So, the correct message is displayed but the chassis type listed is WS-C4510R-E instead of WS-C4510R+E.

Workarounds:

- Place the Supervisor Engine II+10GE in a seven-slot chassis.
- Place a supervisor engine that is supported in a ten-slot chassis. The discrepancy in identifying the chassis type is purely cosmetic.

CSCtl80173

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When you load software images earlier than Cisco IOS Release 12.2(53)SG4, 12.54(SG) or 15.0(1)SG on a redundant WS-C4510R+E or WS-C4507R+E chassis, the active supervisor engines displays the following log message:

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

The active supervisor engine also displays following log message for each linecard slot in the chassis:

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14
```

where *n* is the slot number

If the standby supervisor engine boots, the active supervisor engine displays the following message and reboots:

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

While active supervisor engine is up, no traffic can be handled by the switch.

The two supervisor engines might alternately reboot continuously.

Workaround: Use Cisco IOS Release 12.2(53)SG4, 12.2(54)SG, 15.0(1)SG or later images with WS-C4510R+E and WS-C4507R+E chassis.

CSCtl84092

- When a LAN Base image from Cisco IOS Release 12.2(53)SG3 or earlier is loaded on a WS-C4510R+E or WS-C4507R+E chassis, the system hangs and there is no error message.

Cisco IOS Release 12.2(53)SG3 and earlier are not supported on WS-C4510R+E and WS-4507R+E chassis and should display a valid error message when loaded.

Workaround: Load a LAN Base image from Cisco IOS Release 12.2(53)SG4 and later.

CSCtl89329

- If Supervisor Engine 6-E or Supervisor Engine 6L-E is inserted in a 4507R+E or 4510R+E chassis, ROMMON incorrectly reports the chassis as 4507R-E or 4510R-E.

Workaround: None. CSCtl74638

Resolved Caveats in Cisco IOS Release 12.2(53)SG4

This section lists the resolved caveats in Release 12.2(53)SG4:

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When CX1 or SFP+ are plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None.

CSCtc46340

- If you are using a large custom Webauth login page on a switch running Cisco IOS Release 12.2(53)SG3 or IOS-XE 3.1.0 SG and multiple user are trying to access custom HTML pages, the switch might reload.

Workaround: Unconfigure the customized HTML page to use default internal Webauth pages and reload the switch after changing the configuration. CSCti81874

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

Open Caveats for Cisco IOS Release 12.2(53)SG3

This section lists the open caveats for Cisco IOS Release 12.2(53)SG3:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running
Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- WS-X4548-GB-RJ45V stops supplying inline power to interfaces 1-8 after you perform a switchover to the redundant supervisor engine and expire the watchdog timer.

Workaround: Reload the linecard by entering the hw-module reset command.

CSCti17849

- If you observe a periodic increase in call or packet drops and a constant decrease in free memory available in your switch, you could use the **show memory debug leak** command. However, this command is CPU intensive; it might tear down your call or data session if used on live network.

The **show memory debug leak lowmem** command can work in extremely low memory conditions but might crash the switch due to its very high CPU intensity. It also takes between 20 and 90 minutes to complete.

Workaround: If call or packet drops persist, contact TAC rather than entering these commands on your own. CSCsi48986

- If you are using a large custom Webauth login page on a switch running Cisco IOS Release 12.2(53)SG3 or IOS-XE 3.1.0 SG and multiple user are trying to access custom HTML pages, the switch might reload.

Workaround: Unconfigure the customized HTML page to use default internal Webauth pages and reload the switch after changing the configuration. CSCti81874

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.
(CSCtn68186)

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

**Note**

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:

authentication event server dead action authorize...

authenticaon event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When CX1 or SFP+ are plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None.

CSCtc46340

Resolved Caveats in Cisco IOS Release 12.2(53)SG3

This section lists the resolved caveats in Release 12.2(53)SG3:

- The IP router option may not work with IGMP version 2.

Workaround: None. CSCsv42869

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

CSCsu37834

- The 10Gig uplink on a standby supervisor engine WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR provided the OIR is done quickly, within 5 seconds of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion. CSCsy70428

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. CSCta61825

Workaround: None. CSCtb30327

- A switch crashes if a PBR policy, configured to match on prefix-list(s) instead of ACL(s), is attached to an interface.

This happens provided on the following conditions apply:

- A route map matching on prefix-list is attached to an input interface as a PBR policy.
- A route map for PBR (already attached to an interface) is configured or modified to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map for PBR to only match on ACLs. CSCtg22126

- Under SSH configuration, when using **access-class vty-login in**, you cannot telnet on an interfaces in a VRF. SSH is still avail but not enabled. As documented, if the **vrf-also** keyword is not used in **access-class**, the SSH to interface in VRF will not work.

After upgrading to Cisco IOS Release 12.2(53)SG3, ensure that the **vrf-also** keyword follows any **access-class** under the SSH configuration.

Workaround: None. CSCsv86113

Open Caveats for Cisco IOS Release 12.2(53)SG2

This section lists the open caveats for Cisco IOS Release 12.2(53)SG2:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion.

CSCsy70428

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **auto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. (CSCta61825)

CSCtb30327

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.

- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- A switch crashes if a PBR policy, configured to match on prefix-list(s) instead of ACL(s), is attached to an interface.

This happens provided on the following conditions apply:

- A route map matching on prefix-list is attached to an input interface as a PBR policy.
- A route map for PBR (already attached to an interface) is configured or modified to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map for PBR to only match on ACLs.

CSCtg22126

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.

(CSCtn68186)

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>



Note

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:

authentication event server dead action authorize...

authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.
Workaround: None. (CSCsk66449)
- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.
When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.
For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.
Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.
If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)
- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.
On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.
Workaround: None. (CSCsk52542)
- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.
Workaround: Reinsert the X2. (CSCsk43618)
- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.
When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).
Workaround: None.
Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)
- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.
Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.
Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- When CX1 or SFP+ are plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None.

CSCtc46340

Resolved Caveats in Cisco IOS Release 12.2(53)SG2

This section lists the resolved caveats in Release 12.2(53)SG2:

- A WS-X45-SUP6-E in a Catalyst 4510R chassis running Cisco IOS Release 12.2(52)SGA may fail to boot when 7 or more WS-X4248-RJ45V are installed in the chassis.

This is only seen in Cisco IOS Release 12.2(52)SG.

Workaround: Downgrade to Cisco IOS Release 12.2(50)SG3.

CSCta99577

- A 802.1X port enabled for multi-authentication might not begin learning the MAC address of a successfully authenticated phone.

Workaround: Configure the port in multi-domain mode (rather than multi-auth mode) with the **authentication host-mode multi-domain** command

CSCtb28114

- When using subsecond timers for protocols like HSRP or OSPF, writing to bootflash causes high CPU, and potentially, protocol flapping.

Workaround: Avoid lengthy bootflash operations, like copying large files in IOS.

CSCsw84727

- A PBR policy is not honored on a Supervisor Engine 6 running Cisco IOS Release 12.2(53)SG or 12.2(52)SG. Packets are forwarded through the normal routing table instead of through policy based routing.

This is a side effect of a heavily shared path.

Workaround: None.

CSCtc90702

- Upon upgrading to Cisco IOS Releases 12.2(52)SG, 12.2(52)XO, 12.2(53)SG, or 12.2(53)SG1, if the flash device name differs from the default name *flash:*, you might observe the following message continuously on your console:

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

Workaround: Rename the flash device to the default name *flash:*.

CSCte05909

- MAC learning does not work with Guest VLAN, Wake-on-LAN, and port security. When these features are enabled simultaneously in an interface, MAC learning does not work; none of the packets are forwarded.

Workaround: None.

You will need to disable Wake-on-LAN on the interface.

CSCtc58982

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- After enabling a 802.1X port for Guest VLAN, if you shut down the port connected to the RADIUS server so that the server dies and EAPOL packets are sent on that port, it is authorized in the access VLAN although the server is unreachable.

Workaround: Enter **shut**, then **no shut** on the port.

CSCsz63355

- On a redundant Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, a ping to the FastEthernet1 interface (management interface) from the interface neighbor might fail immediately after an SSO switchover.

Workaround: Clear the ARP table on the neighbor switch.

CSCsy86030

- When a switch enabled for explicit host tracking runs IGMPv3, ports that stopped sending IGMPv3 reports are displayed in the IGMPv3 table until a timeout.

Workaround: Disable explicit host tracking on the affected VLANs.

CSCsz28612

- On a Supervisor Engine V-10GE, on each reload or power off/on, the system clock may lose (decrease) up to 59 seconds.

All software releases up to and including Cisco IOS Releases 12.2(31)SGA9, 12.2(50)SG6 and 12.2(53)SG1 are affected.

Workaround: After rebooting the switch, adjust the system clock with the **clock set** command.

CSCtc65375

- A switch running Cisco IOS Release 12.2(53)SG displays the message

%C4K_EBM-4-HOSTFLAPPING: happening between master loopback port and the source port during layer3 (IPv4 and IPv6) packets loop using ethernet oam (EOAM)

This message does not impact performance.

Workaround: None.

CSCtc26043

- EnergyWise is enabled and you use the **energywise level level recurrence importance importance at minute hour day_of_month month day_of_week** interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
 - Restart when it tries to power a PoE device
 - Power on or off the PoE device at an incorrect time
 - Fail

This occurs when the time change for the next year occurs after the time change for the current year.

Before the time change occurs, use one of these workarounds:

- Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
- Use the **energywise level level recurrence importance importance time-range time-range-name** interface configuration command to reschedule the events.
- Use the **power inline auto** interface configuration command to power on the PoE port.

CSCtc91312

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command.
(CSCsq13477)

- If the router has a (*,G) entry for the group, then a fastdrop entry is not created to block the non-RPF packets from hitting the CPU.

Workaround: Create an ACL to block non-RPF packets from entering non-RPF ports.

CSCta93522

- On a Supervisor Engine 6-E, on each reload or power off/on, the system clock may lose (decrease) up to 59 seconds.

All software releases up to and including Cisco IOS Releases 12.2(31)SGA9, 12.2(50)SG6 and 12.2(53)SG1 are affected.

Workaround: After rebooting the switch, adjust the system clock with the **clock set** command.

CSCtc65375

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- The 4500-E and 4900M switches running IOS Release 12.2(53)SG1 or 12.2(50)SG6 may crash when the only Qos service-policy in a given VLAN is at the VLAN level.

The problem occurs when the following three conditions are met:

- A software-generated or software-switched packet exits an interface (P), which is a member of a VLAN (V).
- The packet is not a high priority; PAK_PRIORITY is not set.
- Of the three possible targets, port P, VLAN V, and port-VLAN PV in the output direction, a qos policy-map is attached only to the VLAN V in the output direction.

Workaround:

- Provided the VLAN-only policy-map has only marking actions., replace the VLAN-only policy-map with a port-VLAN policy-map on all the ports in the VLAN.
- Provided the VLAN-only policy-map has a policing action, retain the VLAN output policymap and attach a queuing action-only output policymap to all the ports in that VLAN.

The port level policy-map should appear as follows.

```
policy-map p1
  class class-default
    bandwidth percent 100
```

CSCte12571

- When running Supervisor Engine II+10GE or Supervisor Engine V-10GE, the X2-10GB-LRM link is down on boot up.

This problem is observed on images later than Cisco IOS Release 12.2(46)SG.

CSCtf26763

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

Open Caveats for Cisco IOS Release 12.2(53)SG1

This section lists the open caveats for Cisco IOS Release 12.2(53)SG1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```

000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby

```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1
```

```
Service-policy output: p1
```

```

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
Police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes

```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface. (CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When the ports connecting a RADIUS server and a client are placed in different VLANs, and you enter the **ip radius source-interface** command and perform two SSO switchovers, the authenticated session is lost.

Workaround: Re-authenticate the client.

CSCsx94066

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion.

CSCsy70428

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- When an access-list is attached to an interface under extreme hardware resource exhaustion, the ACL may not be automatically loaded into the hardware even if hardware resources later become available.

No TCAM entries are available for the new access-list.

Workaround: Manually remove and reapply the ACL after freeing hardware TCAM resources by removing or shortening other classification policies on the switch.

CSCsy85006

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- After enabling a 802.1X port for Guest VLAN, if you shut down the port connected to the RADIUS server so that the server dies and EAPOL packets are sent on that port, it is authorized in the access VLAN although the server is unreachable.

Workaround: Enter **shut**, then **no shut** on the port.

CSCsz63355

- On a redundant Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, a ping to the FastEthernet1 interface (management interface) from the interface neighbor might fail immediately after an SSO switchover.

Workaround: Clear the ARP table on the neighbor switch.

CSCsy86030

- When a switch enabled for explicit host tracking runs IGMPv3, ports that stopped sending IGMPv3 reports are displayed in the IGMPv3 table until a timeout.

Workaround: Disable explicit host tracking on the affected VLANs.

CSCsz28612

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- A 802.1X port enabled for multi-authentication might not begin learning the MAC address of a successfully authenticated phone.

Workaround: Configure the port in multi-domain mode (rather than multi-auth mode) with the **authentication host-mode multi-domain** command

CSCtb28114

- On a Supervisor Engine V-10GE, on each reload or power off/on, the system clock may lose (decrease) up to 59 seconds.

All software releases up to and including Cisco IOS Releases 12.2(31)SGA9, 12.2(50)SG6 and 12.2(53)SG1 are affected.

Workaround: After rebooting the switch, adjust the system clock with the **clock set** command.

CSCtc65375

- When you run Cisco IOS Release 12.2(53)SG1, 12.2(50)SG6, or later releases and configure switchport block multicast on a switch, Layer 2 multicast is not blocked. IPv4 and IPV6 unknown multicast traffic is blocked.

Prior to Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6, the switchport block multicast command blocks IP Multicast, Layer 2 multicast, and broadcast traffic. (CSCta61825)

CSCtb30327

- A switch running Cisco IOS Release 12.2(53)SG displays the message

%C4K_EBM-4-HOSTFLAPPING: happening between master loopback port and the source port during layer3 (IPv4 and IPv6) packets loop using ethernet oam (EOAM)

This message is does not impact performance.

Workaround: None.

CSCtc26043

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- EnergyWise is enabled and you use the **energywise level level recurrence importance importance at minute hour day_of_month month day_of_week** interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
 - Restart when it tries to power a PoE device
 - Power on or off the PoE device at an incorrect time
 - Fail

This occurs when the time change for the next year occurs after the time change for the current year.

Before the time change occurs, use one of these workarounds:

- Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
- Use the **energywise level level recurrence importance importance time-range time-range-name** interface configuration command to reschedule the events.
- Use the **power inline auto** interface configuration command to power on the PoE port.

CSCtc91312

- Upon upgrading to Cisco IOS Releases 12.2(52)SG, 12.2(52)XO, 12.2(53)SG, or 12.2(53)SG1, if the flash device name differs from the default name *flash:*, you might observe the following message continuously on your console:

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

Workaround: Rename the flash device to the default name *flash:*.

CSCte05909

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.

(CSCtn68186)

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>



Note

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:

authentication event server dead action authorize...

authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports.
CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGallInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure vlan dot1q tag native globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- A WS-X45-SUP6-E in a Catalyst 4510R chassis running Cisco IOS Release 12.2(52)SGA may fail to boot when 7 or more WS-X4248-RJ45V are installed in the chassis.

This is only seen in Cisco IOS Release 12.2(52)SG.

Workaround: Downgrade to Cisco IOS Release 12.2(50)SG3.

CSCta99577

- If the router has a (*,G) entry for the group, then a fastdrop entry is not created to block the non-RPF packets from hitting the CPU.

Workaround: Create an ACL to block non-RPF packets from entering non-RPF ports.

CSCta93522

- On a Supervisor Engine 6-E, on each reload or power off/on, the system clock may lose (decrease) up to 59 seconds.

All software releases up to and including Cisco IOS Releases 12.2(31)SGA9, 12.2(50)SG6 and 12.2(53)SG1 are affected.

Workaround: After rebooting the switch, adjust the system clock with the **clock set** command.

CSCtc65375

- When CX1 or SFP+ are plugged into a OneX converter (CVR-X2-SFP10G) in a WS-X4908-10GE, the later requires 1 minute to boot the link.

Workaround: None.

CSCtc46340

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(53)SG1

This section lists the resolved caveats in Release 12.2(53)SG1

- When you configure **switchport block multicast** on a port to block unknown multicast traffic, broadcast traffic is also blocked. Therefore, the port will receive neither unknown multicast or broadcast traffic.

All broadcast traffic (such as ARP request and DHCP discovery) are not received by the port. So, protocols that use such broadcasts stop working.

Workaround:None

CSCta61825

- On a switch with a Supervisor Engine 6-E or 6L-E running Cisco IOS Release 12.2(50)SG1, EIGRP adjacency breaks provided you do either of the following:
 - Enable ip pim sparse-mode on a VLAN interface in a vrf without enabling multicast routing on the vrf.
 - Enable multicast routing on the vrf and setting the STP threshold to infinity.

Workaround: Use static neighbors.

CSCsz61756

- On a switch in redundant SSO mode with Supervisor Engine 6L-E and any of the linecards WS-X4648-RJ45V-E/+E, WS-X4624-SFP and WS-X4606-10GE, the linecard will disable and the following message might appear:

```
%C4K_LINECARD-3-LINECARDWATCHDOGTIMEOUT: Module 2 linecard watchdog has expired.
%C4K_IOSMODPORTMAN-6-MODULEOFFLINE: Module 2 is offline
%C4K_IOSMODPORTMAN-6-MODULEOFFLINE: STANDBY:Module 2 is offline
```

The **show module** command will indicate that the linecard is faulty.

Workaround: Enter **hw-module reset** on the failed module, and reseal the failed module.

CSCsz96231

- Under extremely rare conditions, Supervisor Engine 6-E and 6L-E may stop forwarding traffic. This caveat occurs when a register value is corrupted and you subsequently enable a Layer 3 feature.

Workaround: None (CSCsz48273)

- When a service-policy is attached to a port-channel and that service-policy is configured to match CPU generated packets, the classification statistics do not increment for the CPU generated packets.

Workaround: Configure an access-list to permit the CPU generated packets and apply the ACL to the class-map.

CSCsy43967

- When you edit a policy-map to add a policer configuration, entering either the **do show policy-map interface** or **do show policy-map control-plane** command causes a system reload.

Workaround: Enter either the **show policy-map interface** and **show policy-map control-plane** commands in Exec mode and not in policy-map config mode.

CSCsy43261

- If a policy map is applied on an interface and the interface is inactive (i.e. the port is running in 10GE mode instead of twin gig mode), Supervisor Engines 6-E or 6L-E might crash with Vector 0xD00 when you enter the **show policy-map interface** command.

Workaround: Ensure that the port is active before apply the policy-map or entering the **show policy-map** command.

The command to activate a previously inactive interface is the following:

hw-module module [module number] port-group [group number] select [gigabitethernet]
CSCtb90328

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

Workaround: Manually re-enter all entries with new time settings.

CSCsy27389

- If many ARP entries (47k) exist and you clear the ARP table, the system reloads and the switch crashes with the message:

ROM by abort at PC 0x0

Workaround: None.

Downgrade to Cisco IOS Release 12.2(50)SG3 if needed.

CSCta49512

- If you configure RSPAN on Supervisor Engine 6-E or 6L-E running Cisco IOS Release 12.2(46)SG, CPU utilization will be high when monitored traffic is sent to the destination port.

Workaround: Disable RSPAN.

CSCsu81046

- When you configure a large number of ACLs on a Supervisor 6-E/6L-E and enable statistics, the switch might exhibit high CPU utilization.

Certain applications such as IP Source Guard and QoS enable ACL statistics by default. Configuring such features trigger the high CPU.

High CPU usage is observed through the **show proc cpu** command. The output of the **show platform health** command reveals that the process using a high percentage of CPU is "K5AclCamStatsMan hw".

This issue can occur in any release after Cisco IOS Release 12.2(40)SG.

This issue is resolved in Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6.

Workaround: Reduce the size of the ACL, IPSG, and QoS configurations. If statistics are enabled explicitly for ACLs, disable them with the CLI.

If the high CPU is due to ACLs and IPSG, upgrade to the new software.

If the high CPU is due to the QoS configuration, upgrade the IOS image and enter the **no qos statistics classification** command.

CSCta54369

- If you enable VTP pruning after a switch is moved to VTP version 3, VLAN pruning does not happen on the trunks.

Workaround: Change the VTP version from 3 to version 2 or 1 and then revert to version 3.

CSCsy66803

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, when an 802.1X port configured with PVLAN community VLAN receives a new PVLAN assignment from the AAA server, resetting the configuration on this interface may cause the switch to reload.

Workaround: None.

CSCsz38442

- When the vlan-port state changes on flexlink ports, the following two messages appear on the console:

A syslog warning message "%SM-4-BADEVENT: Event 'forward' is invalid for the current state 'present': pm_vp .."

A traceback error message

This issue happens only on flexlink ports under the following two scenarios:

- You configure flexlink vlan load balancing before changing the port mode of a backup interface to trunk mode.
- Flexlink recovers from per vlan-port error disable states.

Workaround: None

The syslog and Traceback do not impact functionality. Flexlink states end up with correct states and there is no impact on traffic forwarding.

CSCta05317

- Per vlan-port error disable features (dhcp-rate-limit and arp-inspection) do not work on flexlink (without VLAN load balancing). When a violation occurs on the Active link, the corresponding vlan-port will not be error disabled.

The existing per-port error disable (that is, when a violation happens, the entire port will be error disabled) still works on flexlink.

Workaround: Use flexlink with VLAN load balancing.

If you do not want to use vlan load balancing, then enter the **switchport backup interface perfer vlan** command on the Active interface, where vlan z is set to an unused vlan on the system

CSCta76320

- High CPU utilization might be observed on a switch for a prolonged period of time when a large number of packets on a VLAN/SVI are processed by software.

Workaround: None. Functionality is unaffected.

CSCsy32312

- If a switch running Cisco IOS Release 12.2(52)SG receives MPLS packets, SA miss and host learning will cause high CPU.

Workarounds:

- Enter the **mac address-table dynamic group protocols ip other** command.
- Configure a static MAC address.

CSCta09651

Open Caveats for Cisco IOS Release 12.2(53)SG

This section lists the open caveats for Cisco IOS Release 12.2(53)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.
Workaround: Shut down, and then reopen the interface.
(CSCso50921)
- When you delete and recreate an interface, the tacking process is unable to track its state track.
Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)
- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.
Workaround: Do one of the following:
 - Do not attach routers to PVLAN isolated ports.
 - Disable IGMP snooping (either globally or on the VLAN).
 - Do not use a router connected to PVLAN isolated port as a multicast source.
 (CSCsu39009)
- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.
Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)
- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.
Workarounds: Do one of the following:
 - Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
 - Enter **shut** then **no shut** on a 802.1X port.
 (CSCsv05205)
- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.
Workaround: None. (CSCsv07019)
- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.
On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.
Workaround: Do one of the following:
 - Ensure that only one active Layer 3 interface exists on the switch.
 - Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
 - Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.
 (CSCsv28348)
- The IP router option may not work with IGMP version 2.
Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When the ports connecting a RADIUS server and a client are placed in different VLANs, and you enter the **ip radius source-interface** command and perform two SSO switchovers, the authenticated session is lost.

Workaround: Re-authenticate the client.

CSCsx94066

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion.

CSCsy70428

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- When an access-list is attached to an interface under extreme hardware resource exhaustion, the ACL may not be automatically loaded into the hardware even if hardware resources later become available.

No TCAM entries are available for the new access-list.

Workaround: Manually remove and reapply the ACL after freeing hardware TCAM resources by removing or shortening other classification policies on the switch.

CSCsy85006

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, when an 802.1X port configured with PVLAN community VLAN receives a new PVLAN assignment from the AAA server, resetting the configuration on this interface may cause the switch to reload.

Workaround: None.

CSCsz38442

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- After enabling a 802.1X port for Guest VLAN, if you shut down the port connected to the RADIUS server so that the server dies and EAPOL packets are sent on that port, it is authorized in the access VLAN although the server is unreachable.

Workaround: Enter **shut**, then **no shut** on the port.

CSCsz63355

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

Workaround: Manually re-enter all entries with new time settings.

CSCsy27389

- On a redundant Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, a ping to the FastEthernet1 interface (management interface) from the interface neighbor might fail immediately after an SSO switchover.

Workaround: Clear the ARP table on the neighbor switch.

CSCsy86030

- When a switch enabled for explicit host tracking runs IGMPv3, ports that stopped sending IGMPv3 reports are displayed in the IGMPv3 table until a timeout.

Workaround: Disable explicit host tracking on the affected VLANs.

CSCsz28612

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- If a host is authenticated in the data VLAN, the STP state of the VLAN is blocked.

Assuming that you configured authentication open on the port and a host is authenticated on that port, if you unconfigure open auth (no authentication open), the STP state becomes blocked on an authenticated port.

The connected host is authenticated so it should be able to send traffic and the STP state should be Forwarding.

Workaround: Enter **shut**, then **no shut** on the port.

CSCta04665

- On a Layer 2 port (that is, a switchport) of Supervisor Engine II+ thru V-10GE, the **lauto qos voice trust** command auto generates qos trust cos configuration, in addition to other parameters. However, when the port is converted from Layer 2 to Layer 3 with the no switchport command, the **qos trust dscp** command should be generated.

Workaround: When interface mode is changed from Layer2 to Layer3, manually change interface trust state by enter the **cos trust dscp** command.

CSCta16492

- When the vlan-port state changes on flexlink ports, the following two messages appear on the console:

```
A syslog warning message "%SM-4-BADEVENT: Event 'forward' is invalid for the current
state 'present': pm_vp .."
```

```
A traceback error message
```

This issue happens only on flexlink ports under the following two scenarios:

- You configure flexlink vlan load balancing before changing the port mode of a backup interface to trunk mode.
- Flexlink recovers from per vlan-port error disable states.

Workaround: None

The syslog and Traceback do not impact functionality. Flexlink states end up with correct states and there is no impact on traffic forwarding.

CSCta05317

- Per vlan-port error disable features (dhcp-rate-limit and arp-inspection) do not work on flexlink (without VLAN load balancing). When a violation occurs on the Active link, the corresponding vlan-port will not be error disabled.

The existing per-port error disable (that is, when a violation happens, the entire port will be error disabled) still works on flexlink.

Workaround: Use flexlink with VLAN load balancing.

If you do not want to use vlan load balancing, then enter the

switchport backup interface perfer vlan command on the Active interface, where vlan z is set to an unused vlan on the system

CSCta76320

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.

- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- EnergyWise is enabled and you use the **energywise level level recurrence importance importance at minute hour day_of_month month day_of_week** interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
 - Restart when it tries to power a PoE device
 - Power on or off the PoE device at an incorrect time
 - Fail

This occurs when the time change for the next year occurs after the time change for the current year.

Before the time change occurs, use one of these workarounds:

- Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
- Use the **energywise level level recurrence importance importance time-range time-range-name** interface configuration command to reschedule the events.
- Use the **power inline auto** interface configuration command to power on the PoE port.

CSCtc91312

- Upon upgrading to Cisco IOS Releases 12.2(52)SG, 12.2(52)XO, 12.2(53)SG, or 12.2(53)SG1, if the flash device name differs from the default name *flash:*, you might observe the following message continuously on your console:

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

Workaround: Rename the flash device to the default name *flash:*.

CSCte05909

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- A switch may crash while loading BGP routes if the **ip cef accounting non-recursive** command is already configured.

Workaround: Disable the **ip cef accounting non-recursive** command.

(CSCtn68186)

- If you use AAA accounting with the **broadcast** keyword, a switch may either display unpredictable behavior or crash.

Workaround: Do not use AAA accounting with the **broadcast** keyword. CSCts56125

- A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

Additional information on Cisco's security vulnerability policy can be found at the URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

CSCtr91106

- A switch operating as a DHCP server where sessions receive DHCP information from a RADIUS server may experience a crash and DHCP related errors.

Workaround: None. CSCtj48387

- A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>



Note

The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- A switch crashes after displaying the message:

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

provided the following conditions apply:

- A switchport is configured with the following:
authentication event server dead action authorize...
authentication event server alive action reinitialize

- The RADIUS server was down previously, and a port without traffic (for example, a hub with no devices attached) was authorized into the inaccessible authentication bypass (IAB) VLAN without an associated MAC address.

The RADIUS server becomes available again, and the IAB-authorized port transitions to another state.

Workaround: None. CSCtx61557

- When a trunk port is configured with a native VLAN other than VLAN 1, REP packets are not sent on that VLAN.

Workaround: Retain the default setting (VLAN 1) for the native VLAN on trunks ports. CSCud05521

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- If a switch running Cisco IOS Release 12.2(52)SG receives MPLS packets, SA miss and host learning will cause high CPU.

Workarounds:

- Enter the **mac address-table dynamic group protocols ip other** command.
- Configure a static MAC address.

CSCta09651

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.

- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.

- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- High CPU utilization might be observed on a switch for a prolonged period of time when a large number of packets on a VLAN/SVI are processed by software.

Workaround: None. Functionality is unaffected.

CSCsy32312

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- When using subsecond timers for protocols like HSRP or OSPF, writing to bootflash causes high CPU, and potentially, protocol flapping.

Workaround: Avoid lengthy bootflash operations, like copying large files in IOS.

CSCsw84727

Resolved Caveats in Cisco IOS Release 12.2(53)SG

This section lists the resolved caveats in Release 12.2(53)SG:

- When port-security is configured on normal trunks carrying primary and secondary private VLANs, its configuration can be erased from the running-config under the following circumstances:

Entering **shut**, then **no shut** on the port after deleting a secondary VLAN.

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut**, then **no shut** after deleting the VLAN.
- Configure port-security aging time to age out the MAC addresses before entering **shut**, then **no shut**. Then, you can reconfigure port-security on the port only after reloading the switch.

CSCsz73895

- Entering **shut**, then **no shut** on the port after configuring **port-security vp err disable** triggers a violation.

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut**, then **no shut** to recover the port.
- Enter **clear errdisable interface vlan** rather than **shut**, then **no shut**.
- Configure port-security aging time to age out the MAC addresses before entering **shut**, then **no shut**. Reload the switch, then reconfigure port-security.

CSCsy80415

- Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls>

- CSCsq24002
- Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

CSCsx70889

- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

Open Caveats for Cisco IOS Release 12.2(52)XO

This section lists the open caveats for Cisco IOS Release 12.2(52)XO:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1
```

```
Service-policy output: p1
```

```
Class-map: c1 (match-all)
```

```
0 packets<-----It stays at '0' despite of traffic being received
```

```
Match: access-group name fnacl21
```

```
police: Per-interface
```

```
Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.

- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When the ports connecting a RADIUS server and a client are placed in different VLANs, and you enter the **ip radius source-interface** command and perform two SSO switchovers, the authenticated session is lost.

Workaround: Re-authenticate the client.

CSCsx94066

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- If you enable VTP pruning after a switch is moved to VTP version 3, VLAN pruning does not happen on the trunks.

Workaround: Change the VTP version from 3 to version 2 or 1 and then revert to version 3.

CSCsy66803

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion.

CSCsy70428

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#

```

```
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- When an access-list is attached to an interface under extreme hardware resource exhaustion, the ACL may not be automatically loaded into the hardware even if hardware resources later become available.

No TCAM entries are available for the new access-list.

Workaround: Manually remove and reapply the ACL after freeing hardware TCAM resources by removing or shortening other classification policies on the switch.

CSCsy85006

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, when an 802.1X port configured with PVLAN community VLAN receives a new PVLAN assignment from the AAA server, resetting the configuration on this interface may cause the switch to reload.

Workaround: None.

CSCsz38442

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- After a .1X port is enabled for Guest VLAN, if you shut down the port connected to the RADIUS server so that the server goes dead and EAPOL packets are sent on that port, it is authorized in the access VLAN although the server is unreachable.

Workaround: Enter **shut**, then **no shut** on the port.

CSCsz63355

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

Workaround: Manually re-enter all entries with new time settings.

CSCsy27389

- On a redundant Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, a ping to the FastEthernet1 interface (management interface) from the interface neighbor might fail immediately after an SSO switchover.

Workaround: Clear the ARP table on the neighbor switch.

CSCsy86030

- When a switch enabled for explicit host tracking runs IGMPv3, ports that stopped sending IGMPv3 reports are displayed in the IGMPv3 table until a timeout. This behavior didn't exist in Cisco IOS Release 12.2(50)SG.

Workaround: Disable explicit host tracking in the affected VLANs.

CSCsz28612

- On wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

Workaround: Use VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, the IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- When port-security is configured on normal trunks carrying primary and secondary private VLANs, its configuration can be erased from the running-config under the following circumstances:

Entering **shut/no shut** on the port after deleting a secondary VLAN. (CSCsz73895)

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut/no shut** after deleting the VLAN.
- Configure port-security aging time to age out the MAC addresses before entering **shut/no shut**. Then, you can reconfigure port-security on the port only after reloading the switch.

CSCsz73895

Entering **shut/no shut** on the port after configuring **port-security vp err disable** and a violation occurs. (CSCsz80415)

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut/no shut** to recover the port.
 - Configure **clear errdisable interface name vlan [range]** instead of entering **shut/no shut**.
 - Configure port-security aging time to age out the MAC addresses before entering **shut/no shut**. Then, reconfigure port-security on the port after reloading the switch.
- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- EnergyWise is enabled and you use the **energywise level level recurrence importance importance at minute hour day_of_month month day_of_week** interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
 - Restart when it tries to power a PoE device
 - Power on or off the PoE device at an incorrect time
 - Fail

This occurs when the time change for the next year occurs after the time change for the current year.

Before the time change occurs, use one of these workarounds:

- Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
- Use the **energywise level level recurrence importance importance time-range time-range-name** interface configuration command to reschedule the events.
- Use the **power inline auto** interface configuration command to power on the PoE port.

CSCtc91312

- Upon upgrading to Cisco IOS Releases 12.2(52)SG, 12.2(52)XO, 12.2(53)SG, or 12.2(53)SG1, if the flash device name differs from the default name *flash:*, you might observe the following message continuously on your console:

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

Workaround: Rename the flash device to the default name *flash:*.

CSCte05909

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

- With a NEAT configuration on an ASW (Catalyst 4500 series switch) connected to an SSW (Catalyst 3750 series switch) serving as a root bridge and with redundant links between ASW and SSW, the following occur:
 - STP does not stabilize.
 - The SVI (network) is unreachable. If an SVI exists on the ASW, because of the STP flap in the setup as well as the CISP operations, the SVI MAC configuration on the ASW is incorrect.

Workaround: Configure the ASW or any other switch upstream as the root-bridge for all the VLANs. CSCtg71030

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- If a switch running Cisco IOS Release 12.2(52)SG receives MPLS packets, SA miss and host learning will cause high CPU.

Workarounds:

- Enter the **mac address-table dynamic group protocols ip other** command.
- Configure a static MAC address.

CSCta09651

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- When using subsecond timers for protocols like HSRP or OSPF, writing to bootflash causes high CPU, and potentially, protocol flapping.

Workaround: Avoid lengthy bootflash operations, like copying large files in IOS.

CSCsw84727

Resolved Caveats in Cisco IOS Release 12.2(52)X0

This section lists the resolved caveats in Release 12.2(52)X0:

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a switch with Supervisor Engine WS-X45-SUP6-E running Cisco IOS Release 12.2(46)SG or 12.2(50)SG, when traffic is sent out on a 802.1Q trunk port AND on non-native VLANs, locally generated traffic with DSCP 46 is remarked to DSCP 0 before it is sent out.

This behaviour is not observed with traffic passing through the switch.

Workaround: None.

CSCsu01848

- Under normal operation, you will observe the following messages in the logs:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None

CSCsv17545

- Under control plane policing, control plane classes (the classes that are auto created by the **macro global apply system-cpp** command and use predefined ACLs to match traffic) increment both their packet and byte count. So, both counters are non-zero.

In contrast, data plane classes (the classes that are configured manually by user written ACLs), the byte counter increments as expected, but the packet count remains 0.

Workaround: None.

CSCsw16557

- On a Catalyst 4500, if an isolated private VLAN trunk interface flaps, the ingress and egress per-port per-vlan service policies are no longer applied on the port.

This impacts Cisco IOS Releases 12.2(31)SGA08, 12.2(37)SG, 12.2(40)SG, 12.2(44)SG, 12.2(46)SG, 12.2(50)SG, and 12.2(50)SG1.

Workarounds:

For a Classic Series Supervisor Engine, disable and configure QoS on the port.

For example, to configure Gig 2/1 as an isolated private VLAN trunk port, do the following:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# no qos
Switch(config-if)# qos
Switch(config-if)# end
Switch#
```

You can configure the following EEM script to automate this workaround. QoS will be disabled and re-enabled whenever a port flaps.

```
logging event link-status global

event manager applet linkup-reqos
```

```

event syslog pattern "changed state to up"
action 1 cli command "enable"
action 2 cli command "conf t"
action 3 cli command "interface gigabitEthernet 2/1"
action 4 cli command "no qos"
action 5 cli command "qos"

```

On Supervisor Engine 6-E or a Catalyst 4900M switch, remove and reapply the QoS service policy on the impacted VLAN:

```

Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# vlan-range 10
Switch(config-if-vlan-range)# no service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# no service policy input secVlanInPolicy
Switch(config-if-vlan-range)# service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# service policy input secVlanInPolicy
Switch(config-if-vlan-range)# end
Switch#

```

CSCsw19087

- Your standby supervisor engine crashes when you enter the following commands:

```

interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
    priority high
  ip dhcp snooping limit rate 100

```

The problem occurs on redundant Catalyst 4500 series switches that run Cisco IOS Releases 12.2(46)SG or 12.2(50)SG and use one of the following supervisor engines: II Plus, II Plus+10GE, IV, V, or V-10GE.

Workaround: Configure each interface individually.

Explicitly enter the **exit** or **end** commands to exit the **tx-queue** configuration context illustrated above. The short form of the **exit** command (**ex**) does not work. Type the commands **exit** and **end** line by line, rather than copying and pasting a lot of commands.

CSCsx44995

- Provided you enable 1000base-SX Auto-negotiation, some ports might not boot correctly after you reload or reconnect an Intel 1000Base fiber NIC.

The following linecards are affected:

- WS-X4302-GB
- WS-X4306-GB
- WS-X4418-GB
- WS-X4448-GB-SFP
- WS-X4506-GB-T

E-series linecards with SFP, TenGigabit ports using HAMM modules, and WS-C4948 SFP uplinks do not exhibit this problem.

Workarounds: Do one of the following:

- Enter the **shut** then **no shut** commands.
- Re-connect the cable.

CSCsx74970

- When you run an SNMP (getmany) query on cbQosPoliceStatsTable and cbQosREDClassStatsTable with a single SSH window (session), CPU utilization achieves 99 per cent. If you query cbQosPoliceStatsTable and cbQosREDClassStatsTable from 18 SSH sessions, a CPU-HOG error message displays.

Workaround: None, other than stopping the query.

CSCsw89720

- On a supervisor engine running Cisco IOS Release 12.2(50)SG or later releases with one or more ports configured for single-host mode, MAB, and authentication control-direction in, hosts are not authenticated through MAB when a port is configured for single-host mode and you enter the **unidirectional control in** command (Wake-on-LAN).

Workaround: Disable the **authentication control-direction in** command.

If you require **authentication control-direction in**, configure the port for multi-authentication or Multi-Domain Authentication (MDA).

CSCsx98360

- On a redundant switch running Cisco IOS Releases 12.2(50)SG or 12.2(50)SG1 where 802.1X VVID and port security are configured on a port, CDP MAC from the non 802.1X capable Cisco IP phone might not be added to the port security table on the standby supervisor engine.

Workaround: None.

This problem is fixed in Cisco IOS Releases 12.2(50)SG2 and 12.2(52)SG.

CSCsw29489

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 where 802.1X VVID and port security are configured on a port, inserting a non 802.1X capable Cisco IP phone with LLDP capability and a PC behind it may trigger a security violation.

Workaround: Turn off LLDP (on the switch) and the phone (from Call Manager).

This problem is fixed in 12.2(50)SG2 and 12.2(52)SG.

CSCsy21167

- Parity errors in the CPU's cache cause IOS to crash with a crashdump file like the following:

```
Switch# show platform crashdump

VECTOR 0

*** CRASH DUMP ***
02/09/2009 10:10:30
Last crash: 02/09/2009 10:10:30

Build: 12.2(20090206:234053) IPBASE
buildversion addr: 13115584

MCSR: 40000000 <--- non-zero value!
.
```

The key pieces of data are "VECTOR 0" and a MCSR value of 40000000, 20000000, or 10000000.

Workaround: Enter the **show platform cpu cache** command to launch an IOS algorithm that detects and recovers from parity errors in the CPU's cache. You will obtain a running count of the number of CPU cache parity errors that have been successfully detected and corrected on a running system:

```
Switch# show platform cpu cache
```

```
L1 Instruction Cache: ENABLED
L1 Data Cache: ENABLED
L2 Cache: ENABLED
Machine Check Interrupts: 5
L1 Instruction Cache Parity Errors: 3
L1 Instruction Cache Parity Errors (CPU30): 1
L1 Data Cache Parity Errors: 1
```

CSCsx15372

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSC_{su}36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on a bootflash image.

Workaround: Verify the integrity of the image with the `verify /md5` command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSC_{su}37068)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None.

(CSCsw32519)

- Entering **lacp** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None.

(CSCsv91302)

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None.

CSCsy29140

- If you are running Cisco IOS Releases 12.2(46)SG and 12.2(50)SGA on a redundant Catalyst 4500 series switch with Supervisor Engines II+, II+10GE, IV, V or V-10GEs, your standby supervisor engine fails when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

Workaround: Configure every interface individually.

To avoid rebooting the standby supervisor engine, explicitly run the **exit** or **end** command to exit the tx-queue configuration context when working in an interface range. The short form of the exit command **ex** does not work. These commands should be typed line by line; copy/paste will not work.

CSCsx44995

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use AutoQos. CSCsv03316

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them.

(CSCsq74229)

- Ordinarily, you observe the following messages frequently in the logs, which imply no impact to performance:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None. (CSCsv17545)

- When a supervisor fails, the exception crashinfo file is created but not copied to bootflash or slot0 when you configure a switch in RPR mode, even if you have enabled such copying. It may still be copied or examined manually.

The exception crashinfo file feature is not supported in RPR mode.

Workaround: None. (CSCsr66481)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally.

(CSCsq71546)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- On a Catalyst 4500 switch running 12.2(50)SG or 12.2(50)SG1, when 802.1X VVID and port security are configured together on a switch port, inserting a non 802.1x capable Cisco IP phone with a PC behind it may trigger a security violation.

Workaround: None. CSCsv63638

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- AutoQoS cannot be configured on member port(s) of a port-channel.


```
Switch# sh runn int fa 3/1
      channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use AutoQos. CSCsv03316

- Ordinarily, you observe the following messages frequently in the logs, which imply no impact to performance:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None. (CSCsv17545)

- Entering **lACP** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None.

(CSCsv91302)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None.

(CSCsw32519)

- Your standby supervisor engine crashes when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

The problem occurs on redundant Catalyst 4500 series switches that run Cisco IOS Releases 12.2(46)SG or 12.2(50)SG and use one of the following supervisor engines: II Plus, II Plus+10GE, IV, V, or V-10GE.

Workaround: Configure each interface individually.

Explicitly enter the **exit** or **end** commands to exit the **tx-queue** configuration context illustrated above. The short form of the **exit** command (**ex**) does not work. Type the commands **exit** and **end** line by line, rather than copying and pasting a lot of commands.

CSCsx44995

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None.

CSCsy29140

- Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls>

- CSCsq24002

Open Caveats for Cisco IOS Release 12.2(52)SG

This section lists the open caveats for Cisco IOS Release 12.2(52)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.
- Workaround:** None. (CSCsc11726)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When .1X with MDA is set in host mode and guest VLAN is enabled, when you pump traffic from a traffic generator at a high rate, a Security violation is wrongly flagged.

Workaround: None.

CSCsy38640

- When you enter the **show adjacency x.x.x.x internal** command for an adjacency, the packet counters are increment correctly but the byte counters remain 0.

Workaround: None.

CSCsu35604

- When a link in a REP segment connecting two switches fails, 1 out of 3 attempts result in convergence timing exceeding 300ms.

Workaround: None.

CSCsw42967

- When a link fails on a closed REP segment of 16 nodes configured with VLANs on each node, the convergence time exceeds 250ms especially for multicast traffic.

Workaround: None.

This does not impact REP functionality, but it impacts restoration timing. Traffic restoration time after the failure of a REP segment sometimes exceeds 200ms.

CSCsx55704

- On a redundant switch running Cisco IOS Release 12.2(52)SG, after a ports is authorized through 802.1X, the **show dot1x interface statistics** command may display empty values on the standby supervisor engine.

The statistics are displayed properly on the active supervisor.

Workaround: None.

CSCsx64308

- When the ports connecting a RADIUS server and a client are placed in different VLANs, and you enter the **ip radius source-interface** command and perform two SSO switchovers, the authenticated session is lost.

Workaround: Re-authenticate the client.

CSCsx94066

- When multiple streams of CRC errors are encountered on a WS-C4900M chassis configured with OAM monitoring of frame errored seconds, OAM does not report the value of errored frame seconds correctly if you configure the following CLIs:

```

ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low

```

Workaround: Configure a lower value for the low threshold so that the frame errors are seen divided into the expected number of frame errored seconds.

CSCsy37181

- If you enable VTP pruning after a switch is moved to VTP version 3, VLAN pruning does not happen on the trunks.

Workaround: Change the VTP version from 3 to version 2 or 1 and then revert to version 3.

CSCsy66803

- The 10Gig uplink on a standby supervisor WS-X45-SUP6-E stops transmitting or receiving traffic after the old standby engine becomes active through an OIR (if the OIR is done quickly, within 5 seconds) of the active supervisor engine.

Workaround: Reload the active and standby supervisor engine.

While performing OIR of the supervisor engines, the engines must be removed completely before re-insertion.

CSCsy70428

- When you request an on demand Call Home message send without specifying a profile name & the specified module returns an unknown diagnostic result, the following error message displays:

```

Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)

```

Workaround: Specify a profile name when you enter the diagnostic command.

You might want to avoid requesting on demand send for invalid modules. First, enter the **show module** command to check for valid or present modules.

CSCsz05888

- When an access-list is attached to an interface under extreme hardware resource exhaustion, the ACL may not be automatically loaded into the hardware even if hardware resources later become available.

No TCAM entries are available for the new access-list.

Workaround: Manually remove and reapply the ACL after freeing hardware TCAM resources by removing or shortening other classification policies on the switch.

CSCsy85006

- If you simultaneously apply a service-policy to a port in the output direction and a service-policy to a vlan-range under that port in the output direction, the class-map hit counters in the output of the **show policy-map interface** command are wrong.

Workaround: None.

The queue transmit counters as well as the policing statistics (if any) are correct.

CSCsz20149

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, when an 802.1X port configured with PVLAN community VLAN receives a new PVLAN assignment from the AAA server, resetting the configuration on this interface may cause the switch to reload.

Workaround: None.

CSCsz38442

- Packets entering a switch as fragments or with a non-zero fragment offset field are not be subjected to PBR.

Workaround: None.

CSCsz06719 (4500 + 4900, for now)

- After a .1X port is enabled for Guest VLAN, if you shut down the port connected to the RADIUS server so that the server goes dead and EAPOL packets are sent on that port, it is authorized in the access VLAN although the server is unreachable.

Workaround: Enter **shut**, then **no shut** on the port.

CSCsz63355

- When you configure EnergyWise power control on PoE ports with a time-based execution schedule, time entry executes without adjusting for daylight savings time.

Workaround: Manually re-enter all entries with new time settings.

CSCsy27389

- On a redundant Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(52)SG, a ping to the FastEthernet1 interface (management interface) from the interface neighbor might fail immediately after an SSO switchover.

Workaround: Clear the ARP table on the neighbor switch.

CSCsy86030

- When a switch enabled for explicit host tracking runs IGMPv3, ports that stopped sending IGMPv3 reports are displayed in the IGMPv3 table until a timeout. This behavior didn't exist in Cisco IOS Release 12.2(50)SG.

Workaround: Disable explicit host tracking in the affected VLANs.

CSCsz28612

- On wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

This only happens when the switch is running network mobility service protocol (nmosp). It does not happen if the phone is CDP enabled.

Workaround: Use VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS. Specifically, the IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

CSCsz34522

- When port-security is configured on normal trunks carrying primary and secondary private VLANs, its configuration can be erased from the running-config under the following circumstances:

Entering **shut/no shut** on the port after deleting a secondary VLAN. (CSCsz73895)

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut/no shut** after deleting the VLAN.
- Configure port-security aging time to age out the MAC addresses before entering **shut/no shut**. Then, you can reconfigure port-security on the port only after reloading the switch.

Entering **shut/no shut** on the port after configuring **port-security vp err disable** and a violation occurs. (CSCsz80415)

Workarounds:

- Configure error recovery for port-security violation instead of entering **shut/no shut** to recover the port.
 - Configure **clear errdisable interface name vlan [range]** instead of entering **shut/no shut**.
 - Configure port-security aging time to age out the MAC addresses before entering **shut/no shut**. Then, reconfigure port-security on the port after reloading the switch.
- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- EnergyWise is enabled and you use the **energywise level level recurrence importance importance at minute hour day_of_month month day_of_week** interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
 - Restart when it tries to power a PoE device
 - Power on or off the PoE device at an incorrect time
 - Fail

This occurs when the time change for the next year occurs after the time change for the current year.

Before the time change occurs, use one of these workarounds:

- Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
- Use the **energywise level level recurrence importance importance time-range time-range-name** interface configuration command to reschedule the events.
- Use the **power inline auto** interface configuration command to power on the PoE port.

CSCtc91312

- Upon upgrading to Cisco IOS Releases 12.2(52)SG, 12.2(52)XO, 12.2(53)SG, or 12.2(53)SG1, if the flash device name differs from the default name *flash:*, you might observe the following message continuously on your console:

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

Workaround: Rename the flash device to the default name *flash:*.

CSCtc05909

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCtc51948

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policy map), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- When you configure `vlan dot1q tag native` globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

Workaround: Disable native VLAN tagging on the trunk port of the switch using the **no switchport trunk native vlan tag** command.

CSCsz12611

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- When using subsecond timers for protocols like HSRP or OSPF, writing to bootflash causes high CPU, and potentially, protocol flapping.

Workaround: Avoid lengthy bootflash operations, like copying large files in IOS.

CSCsw84727

Resolved Caveats in Cisco IOS Release 12.2(52)SG

This section lists the resolved caveats in Release 12.2(52)SG:

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- On a switch with Supervisor Engine WS-X45-SUP6-E running Cisco IOS Release 12.2(46)SG or 12.2(50)SG, when traffic is sent out on a 802.1Q trunk port AND on non-native VLANs, locally generated traffic with DSCP 46 is remarked to DSCP 0 before it is sent out.

This behaviour is not observed with traffic passing through the switch.

Workaround: None.

CSCsu01848

- Under normal operation, you will observe the following messages in the logs:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None

CSCsv17545

- Under control plane policing, control plane classes (the classes that are auto created by the **macro global apply system-cpp** command and use predefined ACLs to match traffic) increment both their packet and byte count. So, both counters are non-zero.

In contrast, data plane classes (the classes that are configured manually by user written ACLs), the byte counter increments as expected, but the packet count remains 0.

Workaround: None.

CSCsw16557

- On a Catalyst 4500, if an isolated private VLAN trunk interface flaps, the ingress and egress per-port per-vlan service policies are no longer applied on the port.

This impacts Cisco IOS Releases 12.2(31)SGA08, 12.2(37)SG, 12.2(40)SG, 12.2(44)SG, 12.2(46)SG, 12.2(50)SG, and 12.2(50)SG1.

Workarounds:

For a Classic Series Supervisor Engine, disable and configure QoS on the port.

For example, to configure Gig 2/1 as an isolated private VLAN trunk port, do the following:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# no qos
Switch(config-if)# qos
Switch(config-if)# end
Switch#
```

You can configure the following EEM script to automate this workaround. QoS will be disabled and re-enabled whenever a port flaps.

```
logging event link-status global

event manager applet linkup-reqos
event syslog pattern "changed state to up"
action 1 cli command "enable"
action 2 cli command "conf t"
action 3 cli command "interface gigabitEthernet 2/1"
action 4 cli command "no qos"
action 5 cli command "qos"
```

On Supervisor Engine 6-E or a Catalyst 4900M switch, remove and reapply the QoS service policy on the impacted VLAN:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# vlan-range 10
Switch(config-if-vlan-range)# no service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# no service policy input secVlanInPolicy
Switch(config-if-vlan-range)# service policy output primVlanOutPolicy
```

```
Switch(config-if-vlan-range)# service policy input secVlanInPolicy
Switch(config-if-vlan-range)# end
Switch#
```

CSCsw19087

- Your standby supervisor engine crashes when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
switchport voice vlan 505
qos vlan-based
tx-queue 3
priority high
ip dhcp snooping limit rate 100
```

The problem occurs on redundant Catalyst 4500 series switches that run Cisco IOS Releases 12.2(46)SG or 12.2(50)SG and use one of the following supervisor engines: II Plus, II Plus+10GE, IV, V, or V-10GE.

Workaround: Configure each interface individually.

Explicitly enter the **exit** or **end** commands to exit the **tx-queue** configuration context illustrated above. The short form of the **exit** command (**ex**) does not work. Type the commands **exit** and **end** line by line, rather than copying and pasting a lot of commands.

CSCsx44995

- Provided you enable 1000base-SX Auto-negotiation, some ports might not boot correctly after you reload or reconnect an Intel 1000Base fiber NIC.

The following linecards are affected:

- WS-X4302-GB
- WS-X4306-GB
- WS-X4418-GB
- WS-X4448-GB-SFP
- WS-X4506-GB-T

E-series linecards with SFP, TenGigabit ports using HAMM modules, and WS-C4948 SFP uplinks do not exhibit this problem.

Workarounds: Do one of the following:

- Enter the **shut** then **no shut** commands.
- Re-connect the cable.

CSCsx74970

- When you run an SNMP (getmany) query on cbQosPoliceStatsTable and cbQosREDClassStatsTable with a single SSH window (session), CPU utilization achieves 99 per cent. If you query cbQosPoliceStatsTable and cbQosREDClassStatsTable from 18 SSH sessions, a CPU-HOG error message displays.

Workaround: None, other than stopping the query.

CSCsw89720

- On a supervisor engine running Cisco IOS Release 12.2(50)SG or later releases with one or more ports configured for single-host mode, MAB, and authentication control-direction in, hosts are not authenticated through MAB when a port is configured for single-host mode and you enter the **unidirectional control in** command (Wake-on-LAN).

Workaround: Disable the **authentication control-direction in** command.

If you require **authentication control-direction in**, configure the port for multi-authentication or Multi-Domain Authentication (MDA).

CSCsx98360

- On a redundant switch running Cisco IOS Releases 12.2(50)SG or 12.2(50)SG1 where 802.1X VVID and port security are configured on a port, CDP MAC from the non 802.1X capable Cisco IP phone might not be added to the port security table on the standby supervisor engine.

Workaround: None.

This problem is fixed in Cisco IOS Releases 12.2(50)SG2 and 12.2(52)SG.

CSCsw29489

- On a switch running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 where 802.1X VVID and port security are configured on a port, inserting a non 802.1X capable Cisco IP phone with LLDP capability and a PC behind it may trigger a security violation.

Workaround: Turn off LLDP (on the switch) and the phone (from Call Manager).

This problem is fixed in 12.2(50)SG2 and 12.2(52)SG.

CSCsy21167

- Parity errors in the CPU's cache cause IOS to crash with a crashdump file like the following:

```
Switch# show platform crashdump

VECTOR 0

*** CRASH DUMP ***
02/09/2009 10:10:30
Last crash: 02/09/2009 10:10:30

Build: 12.2(20090206:234053) IPBASE
buildversion addr: 13115584

MCSR: 40000000 <--- non-zero value!
.
```

The key pieces of data are "VECTOR 0" and a MCSR value of 40000000, 20000000, or 10000000.

Workaround: Enter the **show platform cpu cache** command to launch an IOS algorithm that detects and recovers from parity errors in the CPU's cache. You will obtain a running count of the number of CPU cache parity errors that have been successfully detected and corrected on a running system:

```
Switch# show platform cpu cache
L1 Instruction Cache: ENABLED
L1 Data Cache: ENABLED
L2 Cache: ENABLED
Machine Check Interrupts: 5
L1 Instruction Cache Parity Errors: 3
L1 Instruction Cache Parity Errors (CPU30): 1
L1 Data Cache Parity Errors: 1
```

CSCsx15372

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command.

This problem is seen only on an interface configured with VRF.

Workaround: None. (CSCsr69187)

- If you configure PVLAN isolated trunk on a switch, and no native VLAN is assigned to the isolated trunk port, you must assign the native VLAN with the **sw private-vlan trunk native vlan** command.

Workaround: Configure the native VLAN for the PVLAN isolated trunk. (CSCsv38137)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on an bootflash image.

Workaround: Verify the integrity of the image with the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu37068)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None.

(CSC_{sw}32519)

- Entering **lACP** or **PAGP** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None.

(CSCsv91302)

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None.

CSCsy29140

- If you are running Cisco IOS Releases 12.2(46)SG and 12.2(50)SGA on a redundant Catalyst 4500 series switch with Supervisor Engines II+, II+10GE, IV, V or V-10GEs, your standby supervisor engine fails when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

Workaround: Configure every interface individually.

To avoid rebooting the standby supervisor engine, explicitly run the **exit** or **end** command to exit the tx-queue configuration context when working in an interface range. The short form of the exit command **ex** does not work. These commands should be typed line by line; copy/paste will not work.

CSCsx44995

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use Auto Qos. CSCsv03316

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- Ordinarily, you observe the following messages frequently in the logs, which imply no impact to performance:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None. (CSCsv17545)

- When a supervisor fails, the exception crashinfo file is created but not copied to bootflash or slot0 .when you configure a switch in RPR mode, even if you have enabled such copying. It may still be copied or examined manually.

The exception crashinfo file feature is not supported in RPR mode.

Workaround: None. (CSCsr66481)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- On a Catalyst 4500 switch running 12.2(50)SG or 12.2(50)SG1, when 802.1X VVID and port security are configured together on a switch port, inserting a non 802.1x capable Cisco IP phone with a PC behind it may trigger a security violation.

Workaround: None. CSCsv63638

- On a redundant WS-X45-Sup6-E or WS-X4516-10G, when a supervisor engine's 10GE uplinks are connected directly to one of the following peer supervisor engines or linecard's 10GE ports, and if this peer engine is running Cisco IOS Release 12.2(50)SG2 or an earlier release, it will report a link flap after the SSO switch-over:

- WS-X4516-10G
- WS-C4948-10GE
- WS-C4900M
- WS-X4904-10GE

Workarounds:

- Enable link debouncing on the affected 10GE peer port.
- If link debouncing is not available in the current IOS revision, upgrade to Cisco IOS Release 12.2(52)SG. Configuration of link debouncing is not required.

CSCsy48647

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- If you configure PVLAN isolated trunk on a switch, and no native VLAN is assigned to the isolated trunk port, you must assign the native VLAN with the **sw private-vlan trunk native vlan** command.

Workaround: Configure the native VLAN for the PVLAN isolated trunk. (CSCsv38137)

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use AutoQos. (CSCsv03316)

- Ordinarily, you observe the following messages frequently in the logs, which imply no impact to performance:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

Workaround: None. (CSCsv17545)

- Entering **lACP** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None.

(CSCsv91302)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None.

(CSCsw32519)

- Your standby supervisor engine crashes when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

The problem occurs on redundant Catalyst 4500 series switches that run Cisco IOS Releases 12.2(46)SG or 12.2(50)SG and use one of the following supervisor engines: II Plus, II Plus+10GE, IV, V, or V-10GE.

Workaround: Configure each interface individually.

Explicitly enter the **exit** or **end** commands to exit the **tx-queue** configuration context illustrated above. The short form of the **exit** command (**ex**) does not work. Type the commands **exit** and **end** line by line, rather than copying and pasting a lot of commands.

CSCsx44995

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None.

CSCsy29140

- When you use a WCCPv2 service group employing promiscuous TCP mode on an interface, the switch redirects GRE traffic to one of the WAAS devices in the group.

Workaround: Remove the WCCP redirection.

If the WAAS device drops this unexpected GRE traffic, the WCCP service group with promiscuous mode cannot be used on the interface. Conversely, if the WAAS device returns the traffic to the switch, the switch routes it normally to the original destination.

CSCsx56922

- Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls>

- CSCsq24002
- Attempting to use the nested policy-map feature on a Catalyst 4900M can cause the switch to reboot. This issue may occur on switches running Cisco IOS Releases 12.2(40)SG, 12.2(44)SG, 12.2(46)SG, 12.2(50)SG-SG5.

This issue is resolved in 12.2(52)SG (and later) and 12.2(50)SG6 (and later) releases.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- On a switch running Cisco IOS 12.2(52)SG, when a port configured with 802.1X enters per vp errdisable mode because of a violation triggered by port security, DAI, DHCP snooping, or BPDU guard, the port's 802.1X sessions are not cleared despite the linkdown.

Workaround: None.

Do not configure 802.1X with other per vp errdisable features.

CSCsx74871

- 10 Gigabit Ethernet uplinks on a standby WS-X45-SUP6-E supervisor engine stop transmitting traffic after becoming active through SSO although the uplink still receives packets.

You cannot restore the uplink by resetting the standby supervisor engine or by changing the interface configuration.

Workaround: Force another SSO switchover.

Occasionally, you might need to perform further switchovers.

CSCsx52834

- AutoQoS cannot be configured on member ports of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in Cisco IOS Release 12.2(40)SG.

Workaround: Manually apply the configuration that would be generated by Auto QoS.

CSCsv03316

- When two WS-X4503+ supervisor engines are installed in a redundant configuration and you enter the **default interface** command on the IOS HTTP server, the WS-X4503+ supervisor engines reboot.

Workaround: Enter the **default interface** command on the WS-X4503+ supervisor engines.

CSCsy46543

- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- During an ISSU upgrade from an earlier release to Cisco IOS Release 12.2(52)SG (and later) or a downgrade from Cisco IOS Release 12.2(52)SG (and later) to an earlier release, the following harmless message (and traceback) is displayed by the PM ISSU client in the older release. Please ignore this message.

```
*Aug 7 14:28:27.167: %PM_ISSU-3-CAPABILITY: STANDBY:Port Manager ISSU client
rejecting capability 2
-Traceback= 10A55FEC 10A56738 104806A0 101498B8 115D5FC8 115D6044 101418FC
10141A24 10141C50 10480A60 104782AC 108E5B84 108E4700 108E3D28 108E143C
108DBBB8
```

Workaround: None. CSCsr85652

Open Caveats for Cisco IOS Release 12.2(50)SG8

This section lists the open caveats for Cisco IOS Release 12.2(50)SG8:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul 9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul 9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul 9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul 9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul 9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul 9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul 9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul 9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul 9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.
- Workaround:** None. (CSCsc11726)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.
(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

The following system message may appear after you enter the **verify** command on an image in bootflash.

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on a bootflash image.

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSC_{su}37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 12.2(54)SG to 12.2(37)SG

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On switches with dual supervisor engines running Cisco IOS Release 12.2(50)SG or later, the Cisco IP phone with CDP port status TLV support is connected to the dot1x port and the PC is connected behind the phone. After the PC is disconnected from behind the phone, disabling dot1x on the port and then reconnecting the PC to the phone causes the host's MAC address not to be synchronized to the standby supervisor engine. If a supervisor switchover is performed while in this state, the host's MAC address would not be present in the new active supervisor's MAC address table and therefore the host might lose connectivity.

bWorkaround: Enter **shutdown**, then **no shutdown** on the interface. This triggers relearning to occur, and a synchronization of the host's MAC to the standby supervisor engine.

CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to primary VLAN on private VLAN trunk ports. However, the traffic is properly classified and the actions configured in policy are applied properly.

Workaround: None.

CSCsy72343

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGallInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.
This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.
Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)
- IGMP snooping entries are active even after you disable IGMP snooping globally.
Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)
- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.
The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.
Workaround: None. (CSCso96660)
- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.
Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)
- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.
Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)
- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).
Workaround: None. (CSCsq99468)
- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.
You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.
Workaround: Unconfigure, and then reconfigure the IFM on the port.

Resolved Caveats in Cisco IOS Release 12.2(50)SG8

This section lists the resolved caveats in Release 12.2(50)SG8:

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.
Workaround: None. (CSCsr95941)
- On Cisco IOS Releases 12.2(50)SG7 and 12.2(50)SG6, if you reload a local switch (Catalyst 4900M or Supervisor Engine 6-E) with [speed] full/[duplex] full configuration on interface Fa1, the link on both sides will be down after bootup.

Workaround: Unconfigure 100/Full, execute **shut/no shut**, then reconfigure 100/Full on the local switch.

CSCtf76196

- A switch fails if you configure a PBR policy to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map to only match on ACL(s).

CSCtg22126

Open Caveats for Cisco IOS Release 12.2(50)SG7

This section lists the open caveats for Cisco IOS Release 12.2(50)SG7:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.
- Workaround:** None. (CSCsc11726)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.
(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)


```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On switches with dual supervisor engines running Cisco IOS Release 12.2(50)SG or later, the Cisco IP phone with CDP port status TLV support is connected to the dot1x port and the PC is connected behind the phone. After the PC is disconnected from behind the phone, disabling dot1x on the port and then reconnecting the PC to the phone causes the host's MAC address not to be synchronized to the standby supervisor engine. If a supervisor switchover is performed while in this state, the host's MAC address would not be present in the new active supervisor's MAC address table and therefore the host might lose connectivity.

Workaround: Enter **shutdown**, then **no shutdown** on the interface. This triggers relearning to occur, and a synchronization of the host's MAC to the standby supervisor engine.

CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to primary VLAN on private VLAN trunk ports. However, the traffic is properly classified and the actions configured in policy are applied properly.

Workaround: None.

CSCsy72343

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- A switch fails if you configure a PBR policy to match on prefix-list(s) instead of ACL(s).

Workaround: Configure the route map to only match on ACL(s).

CSCtg22126

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- On Cisco IOS Releases 12.2(50)SG7 and 12.2(50)SG6, if you reload a local switch (Catalyst 4900M or Supervisor Engine 6-E) with [speed] full/[duplex] full configuration on interface Fa1, the link on both sides will be down after bootup.

Workaround: Unconfigure 100/Full, execute **shut/no shut**, then reconfigure 100/Full on the local switch.

CSCtf76196

Resolved Caveats in Cisco IOS Release 12.2(50)SG7

This section lists the resolved caveats in Release 12.2(50)SG7:

- The 4500-E and 4900M switches running IOS Release 12.2(53)SG1 or 12.2(50)SG6 may crash when the only Qos service-policy in a given VLAN is at the VLAN level.

The problem occurs when the following three conditions are met:

- A software-generated or software-switched packet exits an interface (P), which is a member of a VLAN (V).
- The packet is not a high priority; PAK_PRIORITY is not set.
- Of the three possible targets, port P, VLAN V, and port-VLAN PV in the output direction, a qos policy-map is attached only to the VLAN V in the output direction.

Workaround:

- Provided the VLAN-only policy-map has only marking actions., replace the VLAN-only policy-map with a port-VLAN policy-map on all the ports in the VLAN.
- Provided the VLAN-only policy-map has a policing action, retain the VLAN output policymap and attach a queuing action-only output policymap to all the ports in that VLAN.

The port level policy-map should appear as follows.

```
policy-map p1
  class class-default
    bandwidth percent 100
```

CSCte12571

- When running Supervisor Engine II+10GE or Supervisor Engine V-10GE, the X2-10GB-LRM link is down on boot up.

This problem is observed on images later than Cisco IOS Release 12.2(46)SG.

CSCtf26763

- A PBR policy is not honored on a Supervisor Engine 6 running Cisco IOS Release 12.2(53)SG or 12.2(52)SG. Packets are forwarded through the normal routing table instead of through policy based routing.

This is a side effect of a heavily shared path.

Workaround: None.

CSCtc90702

- In Cisco IOS Releases 12.2(50)SG, 12.2(52)SG and 12.2(53)SG, some GBICs may be deemed incompatible after you upgrade to 12.2(50)SG. The following message may be displayed:

```
%C4K_TRANSCEIVERMAN-3-INCOMPATIBLE: Port Gi5/10: New transceiver (speed
10Gbps) is incompatible with this module
The Gbic is unusable in the switch configuration with the 12.2(50)SG IOS.
```

Workarounds: Do one of the following

- Use a different GBIC.
- Downgrade to Cisco IOS Release 12.2(46)SG.
- Upgrade to Cisco IOS Release 12.2(53)SG2 or 12.2(50)SG7.

CSCtd40838

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- On PVLAN trunk ports, learned MAC addresses age out unconditionally, resulting in flooding not only at the initial phase of frame delivery, but periodically at every MAC age interval. This behavior makes use of the **switchport block unicast** command risky, because it prevents communication.

Workaround: None. However, you cannot enter the **switchport block unicast** command on PVLAN trunk ports.

CSCtd49056

- When port security is configured or have a static MAC address on an isolated trunk port, the adjacencies for the port are resolved on the primary VLAN rather than on the secondary VLAN.

Workaround: None.

CSCtc79119

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.
Workaround: None. (CSCsv59929)
- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG and later versions, if you enter the **clear port-security dynamic interface fastethernet1** command, the switch reloads.
Do not enter this command if port security is not configured on the interface.
Do not enter this command on fa1.
Workaround: None. CSCtb16586
- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.
Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

Open Caveats for Cisco IOS Release 12.2(50)SG6

This section lists the open caveats for Cisco IOS Release 12.2(50)SG6:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1
```

```

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes

```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
```

```
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

```
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on an bootflash image.

Workaround: Verify the integrity of the image with the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On switches with dual supervisor engines running Cisco IOS Release 12.2(50)SG or later, the Cisco IP phone with CDP port status TLV support is connected to the dot1x port and the PC is connected behind the phone. After the PC is disconnected from behind the phone, disabling dot1x on the port and then reconnecting the PC to the phone causes the host's MAC address not to be synchronized to the standby supervisor engine. If a supervisor switchover is performed while in this state, the host's MAC address would not be present in the new active supervisor's MAC address table and therefore the host might lose connectivity.

Workaround: Enter **shutdown**, then **no shutdown** on the interface. This triggers relearning to occur, and a synchronization of the host's MAC to the standby supervisor engine.

CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to primary VLAN on private VLAN trunk ports. However, the traffic is properly classified and the actions configured in policy are applied properly.

Workaround: None.

CSCsy72343

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG and later versions, if you enter the **clear port-security dynamic interface fastethernet1** command, the switch reloads.

Do not enter this command if port security is not configured on the interface.

Do not enter this command on fa1.

Workaround: None. CSCtb16586

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for C4900M, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

Workaround: None.

Despite the different default value, you can configure any value in the time range.

CSCte51948

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGallInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```



```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

- On PVLAN trunk ports, learned MAC addresses age out unconditionally, resulting in flooding not only at the initial phase of frame delivery, but periodically at every MAC age interval. This behavior makes use of the **switchport block unicast** command risky, because it prevents communication.

Workaround: None. However, you cannot enter the **switchport block unicast** command on PVLAN trunk ports.

CSCtd49056

- When port security is configured or have a static MAC address on an isolated trunk port, the adjacencies for the port are resolved on the primary VLAN rather than on the secondary VLAN.

Workaround: None.

CSCtc79119

Resolved Caveats in Cisco IOS Release 12.2(50)SG6

This section lists the resolved caveats in Release 12.2(50)SG6:

- When you run Supervisor Engine 6 with a large number of Layer 3 routes in the system, high CPU utilization may occur when minimal persistent ARP activity exists.

The **show processes cpu** command indicates that Cat4k Mgmt LoPri consumes a significant amount of CPU. The **show platform health** command indicates that K5L3FlcMan FwdEntry, K5L3Unciast IFE Review, and K5L3UnicastRpf IFE Review processes are running above their target utilization.

Note that large amounts of incomplete ARP entries may result from a scanning device or virus.

Workarounds:

- Reduce the number of Layer 3 routes.
- Prevent the ARP activity that triggers the high CPU utilization.

CSCta77487

- When you configure a large number of ACLs on a Supervisor 6-E/6L-E and enable statistics, the switch might exhibit high CPU utilization.

Certain applications such as IP Source Guard and QoS enable ACL statistics by default. Configuring such features trigger the high CPU.

High CPU usage is observed through the **show proc cpu** command. The output of the **show platform health** command reveals that the process using a high percentage of CPU is "K5AclCamStatsMan hw".

This issue can occur in any release after Cisco IOS Release 12.2(40)SG.

This issue is resolved in Cisco IOS Release 12.2(53)SG1 and 12.2(50)SG6.

Workaround: Reduce the size of the ACL, IPSG, and QoS configurations. If statistics are enabled explicitly for ACLs, disable them with the CLI.

If the high CPU is due to ACLs and IPSG, upgrade to the new software.

If the high CPU is due to the QoS configuration, upgrade the IOS image and enter the **no qos statistics classification** command.

CSCta54369

- If many ARP entries (47k) exist and you clear the ARP table, the system reloads and the switch crashes with the message:

```
ROM by abort at PC 0x0
```

Workaround: None.

Downgrade to Cisco IOS Release 12.2(50)SG3 if needed.

CSCta49512

- When using subsecond timers for protocols like HSRP or OSPF, writing to bootflash causes high CPU, and potentially, protocol flapping.

Workaround: Avoid lengthy bootflash operations, like copying large files in IOS.

CSCsw84727

- ARP entries learned on PVLAN SVIs are not aged out even if the **no ip sticky arp** command is configured globally.

ARP entries learned on normal SVIs are unaffected.

Workaround: Clear these ARP entries with the **clear ip arp** command.

CSCtb37718

- When port security and ARP inspection are configured together, the first ARP packet from a host, which is connected to the switch, could bypass the ARP inspection and be bridged out mistakenly.

Workaround: Disable port security.

CSCtb40187

- When you exit policy-map configuration mode without making changes to a policy-map on a switch configured with a service-policy for QoS, configuring an output service policy on an EtherChannel interface causes a link flap.

Workarounds: Configure identical policy-maps with different names so that each EtherChannel has its own policy. This action restricts the effect of this link flap to a limited number of EtherChannels.

CSCsz82795

- When a service-policy is attached to a port-channel and that service-policy is configured to match CPU generated packets, the classification statistics do not increment for the CPU generated packets.

Workaround: Configure an access-list to permit the CPU generated packets and apply the ACL to the class-map.

CSCsy43967

- When a large number of packets on a VLAN/SVI are processed by software, you might observe high cpu is observed as long as there is a large number of packets reaching the cpu.

Workaround: None. Regular functionality is unaffected.

CSCsy32312

Open Caveats for Cisco IOS Release 12.2(50)SG5

This section lists the open caveats for Cisco IOS Release 12.2(50)SG5:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.
(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSC_{su}36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on a bootflash image.

Workaround: Verify the integrity of the image with the `verify /md5` command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102 Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On switches with dual supervisor engines running Cisco IOS Release 12.2(50)SG or later, the Cisco IP phone with CDP port status TLV support is connected to the dot1x port and the PC is connected behind the phone. After the PC is disconnected from behind the phone, disabling dot1x on the port and then reconnecting the PC to the phone causes the host's MAC address not to be synchronized to the standby supervisor engine. If a supervisor switchover is performed while in this state, the host's MAC address would not be present in the new active supervisor's MAC address table and therefore the host might lose connectivity.

Workaround: Enter **shutdown**, then **no shutdown** on the interface. This triggers relearning to occur, and a synchronization of the host's MAC to the standby supervisor engine.

CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to primary VLAN on private VLAN trunk ports. However, the traffic is properly classified and the actions configured in policy are applied properly.

Workaround: None.

CSCsy72343

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG and later versions, if you enter the **clear port-security dynamic interface fastethernet1** command, the switch reloads.

Do not enter this command if port security is not configured on the interface.

Do not enter this command on fa1.

Workaround: None. CSCtb16586

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- LogGallInsufficientFansDetected* messages in the log indicate a fan-tray failure.

- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map** *name*, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard.

It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- When a large number of packets on a VLAN/SVI are processed by software, you might observe high cpu is observed as long as there is a large number of packets reaching the cpu.

Workaround: None. Regular functionality is unaffected.

CSCsy32312

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG5

This section lists the resolved caveats in Release 12.2(50)SG5:

- Under extremely rare conditions, a WS-X45-SUP6-E, WS-X45-SUP6L-E may silently stop forwarding traffic.

This caveat occurs when a register value is corrupted and you subsequently enable a Layer 3 feature.

Workaround: None (CSCsz48273)

Open Caveats for Cisco IOS Release 12.2(50)SG4

This section lists the open caveats for Cisco IOS Release 12.2(50)SG4:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.
- Workaround:** None. (CSCsc11726)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.
(CSCso50921)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- Reconfigure the VLAN load balancing configuration on the desired REP ports.
- Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on an bootflash image.

Workaround: Verify the integrity of the image with the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On switches with dual supervisor engines running Cisco IOS Release 12.2(50)SG or later, the Cisco IP phone with CDP port status TLV support is connected to the dot1x port and the PC is connected behind the phone. After the PC is disconnected from behind the phone, disabling dot1x on the port and then reconnecting the PC to the phone causes the host's MAC address not to be synchronized to the standby supervisor engine. If a supervisor switchover is performed while in this state, the host's MAC address would not be present in the new active supervisor's MAC address table and therefore the host might lose connectivity.

Workaround: Enter **shutdown**, then **no shutdown** on the interface. This triggers relearning to occur, and a synchronization of the host's MAC to the standby supervisor engine.

CSCsw91661

- Class-map hit counters do not increment on the egress policy-map when it is attached to primary VLAN on private VLAN trunk ports. However, the traffic is properly classified and the actions configured in policy are applied properly.

Workaround: None.

CSCsy72343

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG and later versions, if you enter the **clear port-security dynamic interface fastethernet1** command, the switch reloads.

Do not enter this command if port security is not configured on the interface.

Do not enter this command on fa1.

Workaround: None. CSCtb16586

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None. (CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard.

It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- When a large number of packets on a VLAN/SVI are processed by software, you might observe high cpu is observed as long as there is a large number of packets reaching the cpu.

Workaround: None. Regular functionality is unaffected.

CSCsy32312

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.

- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20

IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG4

This section lists the resolved caveats in Release 12.2(50)SG4:

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use Auto Qos. CSCsv03316

- Ordinarily, you observe the following messages frequently in the logs:

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
```

```
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

They imply no impact to performance.

Workaround: None. (CSCsv17545)

- Entering **lACP** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None. (CSCsv91302)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None. (CSCsw32519)

- If you are running Cisco IOS Releases 12.2(46)SG and 12.2(50)SGA on a redundant Catalyst 4500 series switch with Supervisor Engines II+, II+10GE, IV, V or V-10GEs, your standby supervisor engine fails when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
    priority high
  ip dhcp snooping limit rate 100
```

Workaround: Configure every interface individually.

To avoid rebooting the standby supervisor engine, explicitly run the **exit** or **end** command to exit the tx-queue configuration context when working in an interface range. The short form of the exit command **ex** does not work. These commands should be typed line by line; copy/paste will not work.

CSCsx44995

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None. (CSCsy29140)

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

This behavior is seen in Cisco IOS Releases 12.2(50)SG thru 12.2(50)SG3 when the peer device sends a remote fault.

Workaround: Disable auto negotiation at both ends.

(CSCta02425)

- Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy>

CSCsy15227

- Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls>

- CSCsq24002
- Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

CSCsx70889

- AutoQoS cannot be configured on member ports of a port-channel.

```
Switch# sh runn int fa 3/1
      channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in Cisco IOS Release 12.2(40)SG.

Workaround: Manually apply the configuration that would be generated by Auto QoS.

CSCsv03316

- When two WS-X4503+ supervisor engines are installed in a redundant configuration and you enter the **default interface** command on the IOS HTTP server, the WS-X4503+ supervisor engines reboot.

Workaround: Enter the **default interface** command on the WS-X4503+ supervisor engines.

CSCsy46543

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard.

It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- When you downgrade a redundant SUP6-E switch via ISSU from Cisco IOS 12.2(50)SG2, the supervisor uplinks stop carrying traffic. All links remain up.

Workaround: Reload the shelf.



Note A SSO switchover using an earlier release might restore traffic but it would be temporary.

(CSCsz17726)

Open Caveats for Cisco IOS Release 12.2(50)SG3

This section lists the open caveats for Cisco IOS Release 12.2(50)SG3:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.
- Workaround:** None. (CSCsc11726)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

- The following system message may appear after you enter the **verify** command on an image in bootflash.

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 12.2(54)SG to 12.2(37)SG

```
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on an bootflash image.

Workaround: Verify the integrity of the image with the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None. (CSCsw32519)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- Entering **lACP** or **PAGP** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None. (CSCsv91302)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None. CSCsy29140

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- AutoQoS cannot be configured on member ports of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in Cisco IOS Release 12.2(40)SG.

Workaround: Manually apply the configuration that would be generated by Auto QoS.

CSCsv03316

- If you are running Cisco IOS Releases 12.2(46)SG and 12.2(50)SGA on a redundant Catalyst 4500 series switch with Supervisor Engines II+, II+10GE, IV, V or V-10GEs, your standby supervisor engine fails when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

Workaround: Configure every interface individually.

To avoid rebooting the standby supervisor engine, explicitly run the **exit** or **end** command to exit the tx-queue configuration context when working in an interface range. The short form of the exit command **ex** does not work. These commands should be typed line by line; copy/paste will not work.

CSCsx44995

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use Auto Qos. CSCsv03316

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None. (CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- While running Cisco IOS Release 12.2(50)SGI, on a rare occasion, you will observe the following syslog error message even though the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is information only; it does not indicate a potential problem with the line card.

It impacts only the Catalyst 4500-E chassis: the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ linecards.

Workaround: Ignore the warning message; take no action to reset the line card or port(s). There is no need to perform an RMA or submit the line card for EFA.

(CSCsx32444)

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard.

It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- Ordinarily, you observe the following messages frequently in the logs:

```
001298: .Oct 8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
```

```
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

They imply no impact to performance.

Workaround: None. (CSCsv17545)

- When you downgrade a redundant SUP6-E switch via ISSU from Cisco IOS 12.2(50)SG2, the supervisor uplinks stop carrying traffic. All links remain up.

Workaround: Reload the shelf.



Note A SSO switchover using an earlier release might restore traffic but it would be temporary.

(CSCsz17726)

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

This behavior is seen in Cisco IOS Releases 12.2(50)SG thru 12.2(50)SG3 when the peer device sends a remote fault.

Workaround: Disable auto negotiation at both ends.

(CSCta02425)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG3

This section lists the resolved caveats in Release 12.2(50)SG3:

- A Catalyst 4500 E-Series Switch with Supervisor Engine 6-E might crash if you insert/remove a TwinGig converter or boot it with installed TwinGig converters.

TwinGig converters are only supported on E-series supervisors and line cards. This bug does not affect systems without installed converters.

Workaround: None.

Once the switch has booted successfully and has detected all installed TwinGig converters, it is unlikely to crash unless you insert a converter. CSCsz49331

Open Caveats for Cisco IOS Release 12.2(50)SG2

This section lists the open caveats for Cisco IOS Release 12.2(50)SG2:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1
```

```
Service-policy output: p1
```

```
Class-map: c1 (match-all)
 0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only an interface configured with VRF.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

- The following system message may appear after you enter the **verify** command on an image in bootflash.

[illegible]

```
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on an bootflash image.

Workaround: Verify the integrity of the image with the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None. (CSCsw32519)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- Entering **lACP** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None. (CSCsv91302)

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On classic series supervisors and Supervisor Engine 6-E running Cisco IOS Release 12.2(50)SG and later releases, egress traffic is not allowed on ports configured for Wake-on-LAN (through the **authentication control-direction in** command) and Multi-domain Authentication (MDA) (through the **authentication host-mode multi-domain** command) before the port is authorized.

Workaround: None. CSCsy29140

- Class-map hit counters do not increment on the egress policy-map when it is attached to the primary VLAN on a PVLAN trunk ports. However, the traffic is properly classified and the actions configured in the policy are applied properly.

Workaround: None. CSCsy72343

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- AutoQoS cannot be configured on member ports of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in Cisco IOS Release 12.2(40)SG.

Workaround: Manually apply the configuration that would be generated by Auto QoS.

CSCsv03316

- If you are running Cisco IOS Releases 12.2(46)SG and 12.2(50)SGA on a redundant Catalyst 4500 series switch with Supervisor Engines II+, II+10GE, IV, V or V-10GEs, your standby supervisor engine fails when you enter the following commands:

```
interface range GigabitEthernet8/2 - 48
  switchport voice vlan 505
  qos vlan-based
  tx-queue 3
  priority high
  ip dhcp snooping limit rate 100
```

Workaround: Configure every interface individually.

To avoid rebooting the standby supervisor engine, explicitly run the **exit** or **end** command to exit the tx-queue configuration context when working in an interface range. The short form of the exit command **ex** does not work. These commands should be typed line by line; copy/paste will not work.

CSCsx44995

- AutoQoS cannot be configured on member port(s) of a port-channel.

```
Switch# sh runn int fa 3/1
  channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

This problem is first seen in 12.2(40)SG.

Workaround: Manually apply the configuration that is generated by AutoQoS. Do not use Auto Qos. CSCsv03316

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGalInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None. (CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- While running Cisco IOS Release 12.2(50)SGI, on a rare occasion, you will observe the following syslog error message even though the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is information only; it does not indicate a potential problem with the line card.

It impacts only the Catalyst 4500-E chassis: the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ linecards.

Workaround: Ignore the warning message; take no action to reset the line card or port(s). There is no need to perform an RMA or submit the line card for EFA.

(CSCsx32444)

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard.

It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- Ordinarily, you observe the following messages frequently in the logs:

```
001298: .Oct 8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
```

```
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

They imply no impact to performance.

Workaround: None. (CSCsv17545)

- When you downgrade a redundant SUP6-E switch via ISSU from Cisco IOS 12.2(50)SG2, the supervisor uplinks stop carrying traffic. All links remain up.

Workaround: Reload the shelf.



Note A SSO switchover using an earlier release might restore traffic but it would be temporary.

(CSCsz17726)

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

This behavior is seen in Cisco IOS Releases 12.2(50)SG thru 12.2(50)SG3 when the peer device sends a remote fault.

Workaround: Disable auto negotiation at both ends.

(CSCta02425)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG2

This section lists the resolved caveats in Release 12.2(50)SG2:

- Packets for traffic destined to SNAP host might be dropped if the ARP table indicates that the MAC entry is SNAP.

Workarounds:

1. Configure a static ARPA entry for host.
2. Upgrade to a future IOS release containing the fix.

CSCsu90780

- When SPAN is enabled and the SPAN source port is receiving malformed packet such as the error packets produced by collision, the port might stop receiving packets or might replay the packets repeatedly to cause flooding to other ports.

This issue is observed on platforms including WS-C4948 and WS-X4548-GB, and linecards including:

- WS-X4418-GB (Port 3-18)
- WS-X4506-GB-T (RJ45 ports)
- WS-X4424-GB-RJ45
- WS-X4448-GB-RJ45
- WS-X4548-GB-RJ45
- WS-X4524-GB-RJ45V
- WS-X4548-GB-RJ45V

Workaround: Enable packet filtering so that the SPAN session passes only good packets using the command:

```
monitor session 1 filter packet-type good rx
```

CSCsv07168

- On a Catalyst 4948-10GE chassis running IOS Cisco Releases 12.21(31)SGA or 12.2(46)SG, the default transmit queue selection based on IP DSCP value is incorrect. For example, both CS1 and CS5 traffics are passing through transmit queue 1, instead of 1 and 3.

Workaround: Enable and disable global QoS, as follows:

```
switch# conf t
switch(conf)# qos
switch(conf)# no qos
```

CSCsv29945

- If you configure multiple REP segments, pre-emption in one segment brings down all REP segments.

Workaround: None. CSCsv91297

- On a Catalyst 4500 series switch, if an isolated private VLAN trunk interface flaps, the ingress per-port per-vlan policer is no longer applied on the port.

Affected Cisco IOS releases include 12.2(31)SGA08, 12.2(37)SG, 12.2(40)SG, 12.2(46)SG, and 12.2(50)SG.

Workaround: Disable and configure QoS, as follows:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no qos
Switch(config)# qos
Switch(config)# end
Switch#
```

CSCsw19087

- On a Catalyst 4500 redundant switch running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1, when 802.1X VVID and port security are configured together on a switch port, the CDP MAC from the non 802.1X capable Cisco IP phone may not be added to the port security table on the standby supervisor engine.

Workaround: None. CSCsw29489

- Under certain conditions, a Catalyst 4500R chassis with two supervisor engines (Sup II+, Sup IV, or Sup V) may experience a fail over (supervisor switchover) if the keepalive messages from the peer supervisor engine are missing for 162 seconds.

While the problem is happening, the following messages display:

```
%C4K_REDUNDANCY-4-KEEPALIVE_WARNING: STANDBY:Keepalive messages from peer Supervisor
are missing for 162 seconds
%C4K_REDUNDANCY-3-PEER_RELOAD: STANDBY:The peer Supervisor is being reset because
keepalive message(s) not received.
```

Workaround: None. (CSCsw64001)

- A crash occurs when you enter the **show idprom interface FastEthernet 1** command.

Workaround: None. CSCsw77413

- A 10GE uplink on the standby supervisor engine WS-X45-SUP6-E stops transmitting traffic after becoming active through an SSO switchover. However, packets are still received on the uplink.

Traffic from the peer switch is received by the affected switch, but the peer switch will not receive any traffic from the affected switch. This can cause confusing results for protocols like CDP: the affected switch will report the expected CDP adjacencies while the peer switch will not. This can lead to a misdiagnosis of the problem on the peer switch.

You cannot restore the 10GE uplink by resetting the standby supervisor engine or by changing the interface configuration.

Workaround: Force another SSO switchover.

Though unlikely, the problem might recur on a second switchover. A further switchover would then be necessary.

CSCsx52834

- Hosts are not authenticated through MAB when you configure a port for single-host mode (with the **authentication host-mode single-host** command) and Wake-on-LAN (with the **authentication control-direction in** command).

Workarounds: Disable Wake-on-LAN with the **no authentication control-direction in** command.

CSCsx98360

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1, when you configure both 802.1X VVID and port security together on a switch port, then insert a non-802.1X capable Cisco IP phone with LLDP capability and a PC behind it, you might trigger a security violation. The violation is triggered when the PC behind the phone gets authorized on the port before the IP phone sends LLDP packet.

Workaround: Turn off LLDP on the switch and Cisco IP phone from Call Manager.

CSCsy21167

- The linecards WS-X4648-RJ45V-E or WS-X4648-RJ45V+E do not provide PoE power either on a switch bootup or a linecard reset. The non-PoE links still function.

Workaround: Reload the linecard with the **hw-module reset** command.

CSCsy74921

- When using control plane policing, the control plane classes (the classes that are auto created by the **macro global apply system-cpp** command and use the predefined ACLs to match traffic) increment the packet and byte count. This mean that both counters are non-zero.

In contrast, the data plane classes (configured manually by user written ACLs) increment the byte counter, but not the packet count (remains 0).

Workaround: None.

CSCsw16557

Open Caveats for Cisco IOS Release 12.2(50)SG1

This section lists the open caveats for Cisco IOS Release 12.2(50)SG1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the output of the **show policy-map interface fa6/1** command does not display the packets being matched:

```
Switch# show policy-map int fa6/1
```


Service-policy output: p1

```
Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, and then enter the **no shutdown** command on the port that is in UDLD disable state. This does not affect the switch; the port remains in UDLD disable state. Reentering the **shutdown** command, and then entering the **no shutdown** command on the same port will ensure that the error message does not reappear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain are set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

Workaround: Reconnect. (CSCsb11964)

- After upgrading to 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release. The following table reflects this change.

This only affects a switch that has any of the following queues configured as SPAN source in releases prior to 12.2(31)SG and saved to the startup configuration. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF (if it is disabled by hardware exhaustion), enter the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This situation could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- The switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has enabled IP unnumbered. The switch receives packets that require redirection; and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require an IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you enter the **qos account layer2 encapsulation** command.

Workaround: None. (CSCsg58526)

- When hard-coded duplex and speed settings are deleted after an interface shuts down, an **a-** is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message appears and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- You might observe the following error message during an ISSU upgrade to Cisco IOS Release 12.2(37)SG or later images from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When you send traffic on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225 ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a switch reloads.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running configuration.

Workaround: Before removing a line card, delete the statically configured **ip source binding** entries on any of the interfaces on the line card. (CSCsv54529)

- If you configure OFM on an EtherChannel (with at least two interfaces), when you shut or remove the first member that joined the channel, you lose the CFM neighbor.

Workaround: Clear the errors with the **clear ethernet cfm errors** command. (CSCsv43819)

- If you configure PVLAN isolated trunk on a switch, and no native VLAN is assigned to the isolated trunk port, you must assign the native VLAN with the **sw private-vlan trunk native vlan** command.

Workaround: Configure the native VLAN for the PVLAN isolated trunk. (CSCsv38137)

- On a Catalyst 4500 switch running Cisco IOS Release 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the restoration.

Workaround: Shut down, and then reopen the interface.

(CSCso50921)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode do not move to an Unauthorized state when you remove the PVLAN.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down, and then reopen the interface. (CSCsr58573)

- When you delete and recreate an interface, the tacking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- A switch does not accept the **snmp mib target list vrf** command. A switch rejects this command even if the VRF is present in the DUT.

Workaround: None. (CSCsr95941)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable IGMP snooping, the routers connected to the isolated ports display as PIM neighbors.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable IGMP snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to a guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, you will not see the VLAN updates on the other switches in the VTP domain.

Workaround: Configure an ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP and setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enter the **debug management expression evaluator** command.

Workaround: Disable the **debug management expression evaluator** command. (CSCsu67323)

- Egress traffic may not be allowed if you configure 802.1X as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When you configure two MST instances on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may acquire different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify the source of the IP address in each SXP connection configuration to avoid ambiguity.
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this IP address.

(CSCsv28348)

- The IP router option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the line card in place.
- Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change.

(CSCsv44866)

- When you enter the **issu loadversion** command in a redundant chassis, you might observe a traceback accompanied by a “Bad parent VLAN ID” error message.

Workaround: None. (CSCsv59929)

- If you change the mode of the switch port from CFM-supported mode to CFM-unsupported mode, CFM is disabled automatically. When you reset the mode to supported, the CFM state remains Disabled, as observed in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you observe a bulk-sync failure.

CFM is supported in default switch port mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated, and community host ports) and the dot1q-tunnel modes. It is supported on all other switch port modes.

Workaround: Enable CFM on the interface with the Ethernet **cfm enable** command. (CSCsv67507)

- If VLAN load balancing is progressing, and you reconfigure VLAN load balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: Reconfigure VLAN load balancing with a different configuration, by performing the following task:

- a. Reconfigure the VLAN load balancing configuration on the desired REP ports.
- b. Use the **shut** command on any one REP port in the segment to cause a failure in that segment.
- c. Use the **no-shut** on the same port to restore normal REP topology with one ALT port.
- d. Invoke manual preemption on a primary edge port to obtain VLAN load balancing with the new configuration.

(CSCsv69853)

- When you remove an SFP+ from a OneX converter in a X2 slot, it takes approximately 45 seconds for the system to recognize this action. During this time, all commands indicate that the SFP+ is still present. Reinserting the SFP+ in another port or inserting another SFP+ in the same port can cause a “duplicate seeprom” error message.

Workaround: When a log message appears indicating that the SFP+ has been removed, do one of the following:

- Enter any commands for that port.
- Insert an SFP+ in that port.
- Reinsert the removed SFP+ in any other port.

(CSCsv90044)

- The following system message may appear after you enter the **verify** command on an image in bootflash.

```
Catalyst-4507# verify bootflash:cat4500-entervices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entervices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entervices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entervices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entervices-mz.122-37.SG1.
```

This symptom may occur when running Cisco IOS Release 12.2(40)SG or later.

Workaround: Verify the integrity of the image using the **verify /md5** command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSC_{su}36320)

- On Supervisor Engine 6-E and Catalyst 4900M, no output is displayed after you enter the **verify** command without the **/md5** parameter on a bootflash image.

Workaround: Verify the integrity of the image with the `verify /md5` command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Graphics referenced in HTML pages may not be displayed in a user's browser during web authentication.

Workaround: Embed the graphic into the HTML file up to 256 kilobytes (according to RFC 2397).

The following browsers support RFC 2397:

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSC_{su}37834)

- A router may crash when a user with privilege level 15 logs on with the **callback** or **callback-dialstring** attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running Cisco IOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The **callback** or **callback-dialstring** attribute is configured on the AAA server for the user.

Workaround: Do not configure the **callback** or **callback-dialstring** attribute for the user. If you use the **callback-dialstring** attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None. (CSCsw32519)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- Entering **lACP** or **pagp** command on an fa1 management interface in **channel-group x** or **channel-protocol** mode causes the active supervisor engine to reload.

Port-channel functionality is not supported on the fa1 management interface.

This is a configuration error.

Workaround: None. (CSCsv91302)

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not Supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on the console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- When using control plane policing, the control plane classes (the classes which are auto created by the **macro global apply system-cpp** command and use the predefined ACLs to match traffic) increment the packet and byte count. This means that both counters are non-zero.

Instead, the data plane classes (configured manually by user written ACLs) increment the byte counter, but not the packet count (remains 0).

Workaround: None. CSCsw16557

Supervisor Engine 6-E Specific Caveats

- Systems running Cisco IOS Release 12.2(40)SG do not support the handling of .1Q packets for software QoS lookup.

Workaround: None. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service policy.

When an output service policy attaches to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued are subjected to the DBL algorithm. One or more flows that are classified as *belligerent* (flows that do not back off in response to drops because of congestion in the queue) continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time, and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is nondefault (queuing actions are not configured in the class-default class of the policymap), detach and reattach the service policy.

If this happens on the default queue, modifying and resetting some queuing parameters such as bandwidth and shape resolves the problem. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor engine critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to find the cause of the power-down.

- *LogGallInsufficientFansDetected* messages in the log indicate a fan-tray failure.
- *LogRkiosModuleShutdownTemp* messages in the log indicate that the supervisor engine critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E supports a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits a .1X packet on an interface that has an attached egress QoS policy, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original CoS value for a .1X packet cannot be matched by software QoS (according to CSCsk66449). The packet is transmitted with the CoS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured in CSCsk66449, which indicates that the software QoS cannot match a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, no command exists to verify the current operating state.

Workaround: None. You cannot explicitly verify the trusted boundary state. However, you can indirectly ascertain this state:

The trusted boundary feature ensures that the packet's CoS/DSCP value is trusted or not. When the interface is not in a trusted state, the CoS/DSCP fields are forced to zero on a received packet. Because one QoS policy on that interface uses that CoS/DSCP value for classification, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state.

(CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. If you enter the **show policy-map name**, however, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting Cisco IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the class-default class map in a policy map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. This command dictates the size range. (CSCso06422)

- Uplinks go down when upgrading the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switch port and the flow control receive configuration is toggled on 10-Gb port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched but are internally controlled such that on egress the system is generated by the switch itself. This can happen for certain snooping features such as DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN load balancing (VLB) works correctly. When you enter a force-switchover on the switch that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter **shut** followed by **no shut** on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If FlexLink is applied to a pair of EtherChannels, FlexLink configuration may not be applied after a reboot, provided the backup EtherChannel is defined after the FlexLink configuration.

Workaround: Define the backup EtherChannel before applying the **flexlink** command. (CSCsq13477)

- If an EtherChannel is a member of a FlexLink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (FlexLink failure).

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 seconds of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP (IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as inactive. When you allocate the VLAN, the CC-status remains inactive.

You only see this behavior if you initially did not allocate a VLAN before you configure the IFM, and then at a later time allocate the same VLAN.

Workaround: Unconfigure, and then reconfigure the IFM on the port.

- While running Cisco IOS Release 12.2(50)SGI, on a rare occasion, you will observe the following syslog error message even though the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is information only; it does not indicate a potential problem with the line card.

It impacts only the Catalyst 4500-E chassis: the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ linecards.

Workaround: Ignore the warning message; take no action to reset the line card or port(s). There is no need to perform an RMA or submit the line card for EFA.

(CSCsx32444)

- While running Cisco IOS Release 12.2(50)SG or 12.2(50)SG1 and using WS-X4648-GB-RJ45V or WS-X4648-GB-RJ45V+ line cards, on a rare occasion, you will observe the following syslog error message although the PoE line card is functioning correctly:

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
```

This log message is informational only; it does not reflect a potential problem with the linecard. It only impacts the WS-X4648-GB-RJ45V and WS-X4648-GB-RJ45V+ line cards.

Workaround: Ignore the warning message; take no action to reset the linecard or port(s). You do not need to perform an RMA (Return to Manufacturing for Analysis) nor submit the line card for EFA (Engineering Failure Analysis).

(CSCsx32444)

- Hosts are not authenticated through MAB when you configure a port for single-host mode (with the **authentication host-mode single-host** command) and Wake-on-LAN (with the **authentication control-direction in** command).

Workarounds: Disable Wake-on-LAN with the **authentication control-direction in** command.

CSCsx98360

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

This behavior is seen in Cisco IOS Releases 12.2(50)SG thru 12.2(50)SG3 when the peer device sends a remote fault.

Workaround: Disable auto negotiation at both ends.

(CSCta02425)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
```

```
permit icmp 2020::/96 any nd-ns sequence 10
deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG1

This section lists the resolved caveats in Release 12.2(50)SG1:

- A switch may reload unexpectedly. On the console or in the crashinfo file, the following message might appear:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
```

Workaround: Disable NetFlow with one of the following commands on every subinterface for which NetFlow is configured:

```
no ip flow ingress
no ip flow egress
no ip route-cache flow
```

(CSCsq75944)

- When port security is configured on a port connected to a host through an IP phone and the host is disconnected, the MAC address of the host is not removed from the port security MAC address table even if the IP phone and switch support the CDP second port disconnect TLV feature.

Workaround: To remove the MAC address of the host from the port security MAC address table, unconfigure and reconfigure port security on the port. (CSCsr74097)

Open Caveats in Cisco IOS Release 12.2(50)SG

This section lists the open caveats in Cisco IOS Release 12.2(50)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# show policy-map int
FastEthernet3/2

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet

QueueID	Old QueueName	New QueueName
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- When traffic is sent on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225ms.

Workaround: None. (CSCsm30320)

- An IP unnumbered configuration is lost after a reload.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- In SSO mode, when a port-channel is created, deleted, and re-created on an active supervisor engine with the same channel-number, the standby port-channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the portchannel, create a new channel. (CSCsr00333)

- When you configure **ip source binding** statically on an interface, and then remove linecard on which the interface resides, the entries are not removed from the running config.

Workaround: Before removing a linecard, delete the statically configured **ip source binding** entries on any of the interfaces on the line-card. (CSCsv54529)

- If you configure OFM on an Etherchannel (with at least two interfaces), when you shut or remove the first member that joined the channel, the CFM neighbor is lost.

Workaround: Clear the errors with the **clear ethernet cfm errors** command in EXEC mode. (CSCsv43819)

- If PVLAN isolated trunk is configured on a switch, and no native VLAN is assigned to the isolated trunk port, you must assign the native VLAN with the **sw private-vlan trunk native vlan** command.

Workaround: Configure the native VLAN for the PVLAN isolated trunk. (CSCsv38137)

- The standby supervisor engine fails when you configure the **ip multicast helper-map** command. This problem is seen only under a vrf configured interface.

Workaround: None. (CSCsr69187)

- On a Catalyst 4500 switch running 12.2(50)SG, when the access VLAN is deleted and then restored on a port configured with 802.1x multi-auth, authorized 802.1X clients cannot pass traffic because the spanning tree remains in a Disabled state after the access VLAN is restored.

This problem occurs when an 802.1X client is authorized on a multi-auth port. After the access VLAN is deleted, then restored, the client is reauthorized but the spanning tree state of the access VLAN remains Disabled.

Workaround: Shut down then reopen the interface.

(CSCso50921)

- On a switch running Cisco IOS Release 12.2(50)SG, supplicants authorized on PVLAN in multi-auth host mode are not moved to an Unauthorized state when the PVLAN is removed.

This problem occurs only when a port is configured with PVLAN and 802.1X multi-auth.

Workaround: Shut down then reopen the interface. (CSCsr58573)

- When you delete and recreate an interface, the tracking process is unable to track its state track.

Workaround: Reconfigure tracking on the newly created interface. (CSCsr66876)

- The switch does not accept the **snmp mib target list vrf** command. This command is rejected even if the vrf is present in the DUT.

Workaround: None. (CSCsr95941)

- Ping does not execute prior to a posture validation.

Workaround: Reapply the identity policy on the interface with the **permit icmp** command. (CSCsu03507)

- When a PVLAN isolated port is connected to a router serving as a multicast source, and you enable igmp snooping, the routers connected to the isolated ports display as PIM neighbours.

Workaround: Do one of the following:

- Do not attach routers to PVLAN isolated ports.
- Disable igmp snooping (either globally or on the VLAN).
- Do not use a router connected to PVLAN isolated port as a multicast source.

(CSCsu39009)

- When the switch port configured with 802.1X Multi-Domain Authentication (MDA) and Guest VLAN is connected to a non-802.1X supplicant PC through a hub, the port falls back to guest VLAN. Subsequently, it is stuck in the guest VLAN and ignores all EAPOL traffic from another 802.1X supplicant PC connected to the hub.

Workaround: None. (CSCsu42775)

- VTP databases do not propagate through promiscuous trunk ports. If only promiscuous trunks are configured, users will not see the VLAN updates on the other switches in the VTP domain.

Workaround: For VTP database propagation, configure ISL/dot1q trunk port. (CSCsu43445)

- A switch crashes while deleting an expExpressionTable row with SNMP, while setting expExpressionEntryStatus to 6.
- The switch may reload after destroying the expExpressionTable row via SNMP when you enable the **debug management expression evaluator** command.

Workaround: Remove the above debug command. (CSCsu67323)

- When you configure port security with dot1x, the secure dynamic MAC address of the port security MAC address table does not sync after you run ISSU runversion while upgrading to Cisco IOS Release 12.2(50)SG.

Workaround: None (CSCsu67388)

- Egress traffic may not be allowed when 802.1X is configured as a Unidirectional Controlled Port.

Workarounds: Do one of the following:

- Enter **spanning-tree portfast** then **authentication control-direction in** on a 802.1X port.
- Enter **shut** then **no shut** on a 802.1X port.

(CSCsv05205)

- When two MST instances are configured on two switches, MST information is not properly synchronized to the standby on the second switch.

Workaround: None. (CSCsv07019)

- Certain Cisco Trusted Security (CTS) SXP connection configuration may not consistently select the best source IP for each SXP connection.

On a switch with multiple Layer 3 interfaces, if the CTS SXP connection is configured without specifying source IP address and no default SXP source IP address is configured on the box, different SXP connections may pickup different source IP address for each connection.

Workaround: Do one of the following:

- Ensure that only one active Layer 3 interface exists on the switch.
- Specify source the IP address in each SXP connection configuration so there is no ambiguity
- Configure a default SXP source IP address so that the SXP connection without the source IP address will use this source IP address.

(CSCsv28348)

- IP Router Option may not work with IGMP version 2.

Workaround: None. (CSCsv42869)

- When you remove a linecard containing ports configured with igmp snooping while booting a standby supervisor engine, the active supervisor engine does not sync this configuration to the standby supervisor engine as a part of bulk sync. When you reinstall the linecard, the configuration in the active and standby. supervisor engines will differ.

Workaround: Do one of the following:

- Reload the standby switch again with the linecard in place.
- Remove and add the commands back on the active. The standby will pick up this change.

(CSCsv44866)

- The traceback accompanied by a “Bad parent VLAN ID” error message may be seen in a redundant chassis when you enter the **issu loadversion** command.

Workaround: None. (CSCsv59929)

- If the mode of the switchport is changed from CFM supported mode to CFM unsupported mode, CFM is disabled automatically. When the mode changes back to supported mode, the CFM state remains Disabled. You observe this in the running configuration of the interface. If you run **ISSU runversion** from Cisco IOS Release 12.2(44)SG to 12.2(46)SG, you see a bulk-sync failure.

CFM is supported in default switchport mode. CFM is not supported on the PVLAN access modes (promiscuous, isolated and community host ports) and the dot1q-tunnel modes. It is supported on all other switchport modes.

Workaround: Enable CFM on the interface with the ethernet **cfm enable** command. (CSCsv67507)

- If VLAN Load Balancing is progressing, and you reconfigure VLAN Load Balancing to reflect different blocking ports, manual preemption does not occur.

Workaround: To reconfigure VLAN Load Balancing with a different configuration, do the following:

- Reconfigure the VLAN Load Balancing configuration on the desired REP ports.
- Shut** any one REP port in the segment to cause a failure in that segment.
- No-shut** that port to restore normal REP topology with one ALT port.

- (CSCsv69853)

- Workaround:** When a log message appears indicating that the SFP+ has been removed , do one of the following:

- (CSCsv90044)

- [illegible]

Workaround: Verify the integrity of the image using the `<CmdBold>verify /md5</noCmdBold>` command. Compare the resultant MD5 signature with the signature posted on CCO for that image.

(CSCsu36320)

- Workaround:** Verify the integrity of the image with the `verify /md5` command. Compare the resultant MD5 signature with the signature posted on CCO for that image. (CSCsu37068)

- Workaround:** Embed the graphic into the HTML file up to 256 Kilobytes according to RFC 2397.

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- A router may crash when a privilege-level 15 user logs on with the callback or callback-dialstring attribute.

This problem is seen on all Catalyst 4500 or 4900 chassis running CiscoIOS Release 12.2.(50)SG. The problem occurs when the following conditions are present:

- The router is configured with AAA authentication and authorization.
- The AAA server runs CiscoSecure ACS 2.4.
- The callback or callback-dialstring attribute is configured on the AAA server for the user.

Workarounds: Do not configure the callback or callback-dialstring attribute for the user. If you use the callback-dialstring attribute in the TACACS+ profile, ensure that the NULL value is not configured. (CSCei62358)

- When you attempt an ISSU upgrade or downgrade between Cisco IOS Release 12.2(50)SG and 12.2(44)SG or 12.2(46)SG, the switch displays a traceback.

Workaround: None. (CSCsw32519)

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the global RADIUS and IP device tracking commands:

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

Workaround: None. (CSCsw14005)

- Entering the channel-group x mode or channel-protocol followed by **lacp** or **pagp** command on an fa1 management interface causes the active supervisor engine to reload.

Port-channel functionality is not supported on the management interface.

This is a configuration error.

Workaround: None. (CSCsv91302)

- When using dynamic policy installation for a client or host that is authenticated on a secure port, the traffic from the client is not permitted even though the **permit ip any any** command is specified as the dynamic policy for the client.

This occurs only if the following conditions are satisfied:

- Multi-host mode configured on the port with the **authentication host-mode multi-host** command.
- Default ACL (the IP access-list) configured on the interface specifies **deny ip any any**.
- Dynamic policy authorization for the client specifies **permit ip any any**.

Workaround: None.

CSCsz63739

Not supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

Workaround: None. (CSCso93282)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- When using control plane policing, the control plane classes (the classes which are auto created by the **macro global apply system-cpp** command and use the predefined ACLs to match traffic) increment the packet and byte count. This mean that both counters are non-zero.

Instead, the data plane classes (configured manually by user written ACLs) increment the byte counter, but not the packet count (remains 0).

Workaround: None. CSCsw16557

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workaround: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGalInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- If *burst* is not explicitly configured for a single-rate policer, the **show policy-map** command displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you specify a DBL action for the 'class-default' class-map in a policy-map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. The size range is dictated by the **queue-limit** command. (CSCso06422)

- Uplinks go down when upgrading the rommon of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the ACTIVE supervisor engine is running IOS, the STANDBY supervisor engine is in rommon, and the STANDBY's rommon is upgraded from version 0.34 or to a later version. The upgrade process will cause the uplinks on the STANDBY supervisor engine to go down but the ACTIVE supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisors with the redundancy reload shelf command.
- Power-cycle the STANDBY supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switchport and the flow control receive configuration is toggled on 10G port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched through the switch but are internally controlled such that on egress the system generated by the switch itself. This can happen for certain snooping features like DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- Initially, REP configured with VLAN Load Balancing (VLB) works correctly. When you enter a force-switchover on the switch, that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter shut, then no-shut on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- If flexlink is applied to a pair of etherchannels, then flexlink config may not be applied after a reboot, if the backup EtherChannel is defined after the flexlink configuration.

Workaround: Define the backup etherchannel before applying the flexlink command. (CSCsq13477)

- If an etherchannel is a member of a flexlink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (flexlink failure)

Workaround: None. (CSCsq99468)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 secs of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them. (CSCsq74229)

- When a CFM Inward Facing MEP(IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as **Inactive**. Then, you allocate the VLAN, the CC-status remains **Inactive**.

You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

Workaround: Unconfigure, then reconfigure the IFM on the port.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

- On a Catalyst 4900M switch, when you use a WS-X4908-10GE card with CVR-X2-SFP twin gig converters, the giga ports do not link up to the peer device that sends a remote fault. The **show int status | inc gi x/y** command indicates notconnect.

Similar behavior is observed with Supervisor Engine 6-E uplinks and the WS-X4706-10GE line card.

This behavior is seen in Cisco IOS Releases 12.2(50)SG thru 12.2(50)SG3 when the peer device sends a remote fault.

Workaround: Disable auto negotiation at both ends.

(CSCta02425)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(50)SG

This section lists the resolved caveats in Release 12.2(50)SG:

- After a data device is authorized (with dot1x or MAB) on a port configured with Multi-Domain Authentication (MDA), changing the access VLAN causes traffic loss for this device even if no device is connected on the port. It does *not* affect the traffic from the voice device connected to the port.

Workaround: Enter the **shutdown**, then **no shutdown** commands on the interface after changing the access VLAN on the port. (CSCsk45969)

- When IPv4 routes are advertised by RTR2 to RTR3 over IPv6 peering, the first 32 bits of RTR2's IPv6 address is converted to an IPv4 address. This IPv4 address is advertised as the nexthop address to RTR3. If this address results in a Martian address, then RTR3 will ignore the BGP update message, and will not learn the IPv4 routes.

Configuring an inbound routemap on RTR3 to override the nexthop address advertised by RTR2 does not avoid this problem because the BGP update message is ignored.

Workaround: Configure an outbound routemap on RTR2 to explicitly set the IPv4 nexthop address rather than allow the protocol to derive it implicitly. (CSCsk65139)

- With CFM, if the VLAN associated with the service instance/MEP is allocated after the Inward Facing MEP (IFM) is configured on an interface whose status is **down**, the IFM CC status remains **inactive** in the output of the **show ethernet CFM maintenance local** command. Also, the CFM remote neighbor is not seen.

This behavior is only seen when VLAN is allocated after the IFM is configured.

Workaround: Unconfigure with the **no ethernet cfm mep level mpid vlan** command, then reconfigure the IFM with the **ethernet cfm mep level mpid vlan** command on the port after the VLAN is allocated. Verify that the C-Status of the IFM is Active with the **show ethernet cfm maintenance-points local** command. (CSCsm85460)

- Occasionally, if a PC continues to send traffic behind an 802.1X capable phone that is plugged into a port configured with MDA (Multi-Domain Authentication), MAB (MAC Authentication Bypass) and port security, a 802.1X security violation is triggered if the port observes traffic from the PC before the phone is fully authorized on the port.

Workaround: Authenticate the phone before plugging a PC behind the phone. (CSCsq92724)

- After CFM is disabled globally and a switch is reloaded with the CFM configuration, and after CFM is enabled globally, CFM are inactive, causing a loss of CFM neighbors.

Workarounds: Do one of the following:

- Reapply the CFM configuration; remove and re-add the MEPs configured on all the interfaces of the switch.
- Deallocate CFM service VLANs. Then reallocate them.

(CSCsq90598)

- The **show ip cache verbose flow** command does not display the AS path information, when netflow aggregation for origin-as is configured.

Workaround: None. (CSCsq63572)

- When policer, shape, or shape values are specified as a percentage of link bandwidth on a policy and the interface on which the policy is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer, shape, or bandwidth value might not correspond to the new forced speed.

Service policy has to be configured with percentage police, shape, or share values and the link speed is forced to a specific values. For example:

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape, or shape values rather than percentage values. For example:

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- The message “**Module M linecard watchdog has expired**” appears when the switch boots. The message may appear when a linecard boots, depending on how the hardware has powered-up. **Workaround:** Reset the linecard. (CSCsq21215)
- Percentage based input policer on an interface with non-default speed doesn't work after the system reloads.

Workaround: Remove and re-apply the service-policy on the interface.

(CSCsq79073)

- When policer or shape values are specified as a per cent of link bandwidth on a policy and the interface on which they are attached is forced to a specific speed using the **speed 10/100/1000** command, the applied policer or shape value might correspond to the new forced speed.

Example:

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Use either the **speed auto 10/100/1000** command or the absolute policer or shape values instead of percentage values.

Example:

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- Channel unbundles and re-bundles when a policy map with per cent based actions is shared between channel member ports and another standalone port, and the standalone port is modified from Layer 2 to Layer 3 or Layer 3 to Layer 2. **Workaround:** None. (CSCso54096)
- Performing a default interface operation on an interface with auto-QoS enabled results in an error message and the loss of the auto-QoS configuration. For example, the following sequence of operation results in a loss of the configuration:

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

Workaround: Replace the **default interface** command with the following:

```
config# interface interface-number
config-if# switchport
```

(CSCsq47116)

- Manual Pre-emption is disallowed after you modify a set of blocked VLANs with REP and VLAN load balancing configured.

Workaround: Intentionally fail the link between two switches by physically pulling the cable or shutting down the interface. Then, return the links to a normal condition. This is followed by delayed preemption, which you might have already configured. (CSCsm91997)

- In SSO mode, when you add, remove, or modify service-policies to port-channel members, you see the following traceback on both the active and standby supervisor engine:

```
03:50:00: %SM-4-BADEVENT: STANDBY:Event 'bundle_sync' is invalid for the current state
'COLLECTING_DISTRIBUTING': lacp_mux Gi7/7 - mux
-Traceback= 10B97B80 10B98294 10189F78 1038FE0C 103944FC 1055E420 1055C4B8 10A2C28C
10A2AE88 10A2A4B0 10A27A18 10A225E8 1059E824 10595AAC
```

Workaround: None. CSCso23786)

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

Workaround: Unconfigure any generic QoS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

(CSCsq84796)

- ifindex persistency fails to work when you change the version of software running on the switch to or from Cisco IOS Release 12.2(46)SG. The **show snmp mib ifmib ifindex** command might display interface names incorrectly.

Workaround:

Dual-sup upgrade (ISSU) - Between 12.2(46)SG and other releases

Follow the ISSU process without any changes. Adhere to the following items during the upgrade:

- Do not save the configuration file to nvram explicitly with **write memory** or an equivalent command. The **issu commitversion** command saves the configuration to nvram, which restores the ifIndices stored in nvram.
- Do not enter the **issu abortversion** command during the upgrade process.

Single Supervisor Upgrade - Upgrade from Cisco IOS Release 12.2(44)SG1 or prior to 12.2(46)SG & Downgrade from 12.2(46)SG to 12.2(44)SG1 or prior

For the software versions described in the previous section, observe that the software version is changing from version-a to version-b, with the switch currently running version-a.

Perform the following steps:

- While running version-a, delete the file containing ifIndices with the **del nvram:ifIndex-table.gz** command.



Note

Ensure that you do not initiate saving of the configuration file with **write nvram** or a similar command after step 1):

- Reload the switch so that it runs version-b after reloading.
- While the switch is running version-b, regenerate the file containing ifIndices by saving the configuration with the **write memory** command.

Single Supervisor Upgrade - Upgrade from Cisco IOS Release 12.2(46)SG to 12.2(50)SG or later

1. While running 12.2(46)SG, save the configuration to a file in bootflash.

```
Switch# copy running-config bootflash:oldconfig
```

2. Erase the configuration stored in nvram.

```
Switch# erase nvram:
```

3. Delete the file containing the ifIndices.

```
Switch# del nvram:ifIndex-table.gz
```

4. Reload the switch so that it runs Cisco IOS Release 12.2(44)SG1 or a prior release after reloading.
5. While the switch is running Cisco IOS Release 12.2(44)SG1, regenerate ifIndices by doing the following:
 - Enable the ifIndex persistence feature.
 - Enter the **write memory** command to save the generated ifIndices to nvram.
6. Upgrade to Cisco IOS Release 12.2(50)SG or a later release. While the switch is running release 12.2(50)SG or later, load the configuration saved in step 1 from bootflash with the **copy bootflash:oldconfig running-config** command.
7. Save your configuration to nvram with the **write memory** command.

(CSCsv85746)

- When you use a Catalyst 4500 series switch with Supervisor Engine 6-E with an output service policy configured on an interface, you observe output drops due to a queue full condition when you enter shut/no shut on a different interface that also has the same output service policy applied.

This issue is open in Cisco IOS Releases 12.2(40)SG, 12.2(44)SG and 12.2(46)SG.

This issue is resolved in 12.2(50)SG.

Workaround: Do not use the qos autoqos macro.

When a policy-map is shared on more than one target, it should not use any percentage based actions; police, shape, and bandwidth actions must use absolute values. This requires a different policy-map for each of the four interface speeds supported on the switch - 10M, 100M, 1G, and 10G. So, rather than having a single policy-map as enabled through percentage-based actions, you must create four distinct policy-maps. This applies to all shared policy-maps, independent of direction of service-policy.

(CSCsr12142)

- Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the workarounds section of this advisory.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp>

CSCsr29468

- Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp>
CSCsk64158

- Symptoms: SSLVPN service stops accepting any new SSLVPN connections.
Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

CSCso04657

- IPv6 MLD entries are active even if an IPv6 MLD related configuration does not exist.

Workaround: Unconfigure all generic QOS policies from the system. (CSCsq84853)

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(47)SG, if you configure the switch port connecting to the AAA server as a Layer 2 interface with SVI enabled on the access VLAN, any MDA (Multi-domain Authentication) port configured with port security and spanning-tree portfast might experience an 802.1X security violation when an 802.1X enabled phone tries to authenticate on the MDA port.

Workarounds:

- a. Disable port security on the port, or connect the switch to the AAA server through a standard Layer 3 port.
- b. Disable spanning-tree portfast.

(CSCsq62342)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. (CSCsk67395)

- If a redundant switch is in SSO mode or during an ISSU upgrade/downgrade, and the standby supervisor is running IOS software release 12.2(44)SG or 12.2(46)SG, when you enter the **auto qos voip trust** command on an interface with an attached service-policy, the standby supervisor engine reboots.

Workaround: Remove all service-policies from the interface before entering the **auto qos voip trust** command.

CSCsq37471

- Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In

some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24>
CSCsv04836

Open Caveats in Cisco IOS Release 12.2(46)SG

This section lists the open caveats in Cisco IOS Release 12.2(46)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# show policy-map int
FastEthernet3/2

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.
(CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- If an Cisco IP Phone has an supplicant attached, upon reloading a DUT port configured with MDA and attached to phones and supplicants, the port will not pass traffic. Phone will in an unknown state.

Problem is not observed if the phone is a stand alone device.

Workarounds: Powercycle the Cisco IP phone. (CSCsk81297)

- After a data device is authorized (thru dot1x or MAB) on a port configured with Multi-Domain Authentication (MDA), changing the access VLAN causes traffic loss for this device even if no device is connected on the port. It does *not* affect the traffic from the voice device connected to the port.

Workaround: Enter the **shutdown**, then **no shutdown** commands on the interface after changing the access VLAN on the port. (CSCsk45969)

- When traffic is sent on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225ms.

Workaround: None. (CSCsm30320)

- Manual pre-emption is disallowed after you modify a set of blocked VLANs configured with REP and VLAN load balancing.

Workaround: Cause the link between two switches to fail by physically pulling the cable or shutting down the interface. Then, return the links to a normal condition. This is followed by delayed preemption, which you might have already configured. (CSCsm91997)

- Occasionally, if a PC continues to send traffic behind an 802.1X capable phone that is plugged into a port configured with MDA (Multi-Domain Authentication), MAB (MAC Authentication Bypass) and port security, a 802.1X security violation is triggered if the port observes traffic from the PC before the phone is fully authorized on the port.

Workaround: Authenticate the phone before plugging a PC behind the phone. (CSCsq92724)

- An IP unnumbered configuration is lost after a reload.

Workarounds: Do one of the following:

- After a reload, copy the startup-config to the running-config.
- Use a loopback interface as the target of the **ip unnumbered** command.
- Change the CLI configuration so that during bootup the router port is created first.

(CSCsq63051)

- After CFM is disabled globally and a switch is reloaded with the CFM configuration, and after CFM is enabled globally, CFM are inactive, causing a loss of CFM neighbors.

Workarounds: Do one of the following:

- Reapply the CFM configuration; remove and re-add the MEPs configured on all the interfaces of the switch.
- Deallocate CFM service VLANs. Then reallocate them.

(CSCsq90598)

- In SSO mode, when a port-channel is created, deleted, and re-created on an active supervisor engine with the same channel-number, the standby port-channel state goes out of sync. After a switch over, the following message displays:

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the portchannel, create a new channel. (CSCsr00333)

- For ISSU-enabled redundant supervisor engines, ifindex persistency fails to work when you upgrade from Cisco IOS Release 12.2(44)SG (or earlier) to 12.2(46)SG or later. The **show snmp mib ifmib ifindex** command might display interfaces names incorrectly.

Workaround: Update the configuration during ISSU with **issu commitversion**. This is the normal process. Do *not* save the configuration explicitly with **write nvram**. (CSCsv85746)

- ifindex persistency fails to work when you change the version of software running on the switch to or from Cisco IOS Release 12.2(46)SG. The **show snmp mib ifmib ifindex** command might display interface names incorrectly.

Workaround:

Dual-sup upgrade (ISSU) - Between 12.2(46)SG and other releases

Follow the ISSU process without any changes. Adhere to the following items during the upgrade:

8. Do not save the configuration file to nvram explicitly with **write memory** or an equivalent command. The **issu commitversion** command saves the configuration to nvram, which restores the ifIndices stored in nvram.
9. Do not enter the **issu abortversion** command during the upgrade process.

Single Supervisor Upgrade - Upgrade from Cisco IOS Release 12.2(44)SG1 or prior to 12.2(46)SG & Downgrade from 12.2(46)SG to 12.2(44)SG1 or prior

For the software versions described in the previous section, observe that the software version is changing from version-a to version-b, with the switch currently running version-a.

Perform the following steps:

1. While running version-a, delete the file containing ifIndices with the **del nvram:ifIndex-table.gz** command.



Note Ensure that you do not initiate saving of the configuration file with **write nvram** or a similar command after step 1):

2. Reload the switch so that it runs version-b after reloading.
3. While the switch is running version-b, regenerate the file containing ifIndices by saving the configuration with the **write memory** command.

Single Supervisor Upgrade - Upgrade from Cisco IOS Release 12.2(46)SG to 12.2(50)SG or later

1. While running 12.2(46)SG, save the configuration to a file in bootflash.
Switch# **copy running-config bootflash:oldconfig**
2. Erase the configuration stored in nvram.
Switch# **erase nvram:**
3. Delete the file containing the ifIndices.
Switch# **del nvram:ifIndex-table.gz**
4. Reload the switch so that it runs Cisco IOS Release 12.2(44)SG1 or a prior release after reloading.
5. While the switch is running Cisco IOS Release 12.2(44)SG1, regenerate ifIndices by doing the following:
 - Enable the ifIndex persistence feature.
 - Enter the **write memory** command to save the generated ifIndices to nvram.
6. Upgrade to Cisco IOS Release 12.2(50)SG or a later release. While the switch is running release 12.2(50)SG or later, load the configuration saved in step 1 from bootflash with the **copy bootflash:oldconfig running-config** command.
7. Save your configuration to nvram with the **write memory** command.

(CSCsv85746)

Not supported on Supervisor Engine 6-E

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with HWCOPP (HW Control Plane Policing).

Workaround: None. (CSCso93282)

- The **show ip cache verbose flow** command does not display the AS path information, when netflow aggregation for origin-as is configured.

Workaround: None. (CSCsq63572)

- During an ISSU upgrade or downgrade from v122_31_sg_throttle to v122_46_sg_throttle, the following error message displays on console of the active supervisor engine:

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

Workaround: None. (CSCso68331)

- When using control plane policing, the control plane classes (the classes which are auto created by the **macro global apply system-cpp** command and use the predefined ACLs to match traffic) increment the packet and byte count. This means that both counters are non-zero.

Instead, the data plane classes (configured manually by user written ACLs) increment the byte counter, but not the packet count (remains 0).

Workaround: None. CSCsw16557

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workaround: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or bandwidth value might not correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGallInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. (CSCsk67395)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map command** displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- Executing the **default interface** command twice on a port configured with the cisco-phone macro displays the back trace.

Workaround: Remove the configuration line by line without entering the **default interface** command. (CSCsj23103)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as Unknown. After booting IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- If you configure a QoS policy with queuing actions (like sharing and shaping) on WS-X4648-RJ45V-E (PoE) and WS-X4648-RJ45V+E (Premium PoE with 30 W per port) linecards, the sharing and shaping percentage error increases to 3 percent after an SSO switch over.

Workaround: Do one of the following:

- Remove the service-policy from the interface and reapply the configuration with the **[no] service-policy {input/output}** command.
- Enter the **shutdown** then **noshutdown** commands.

(CSCsm45156)

- When you specify a DBL action for the 'class-default' class-map in a policy-map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. The size range is dictated by the **queue-limit** command. (CSCso06422)

- When IPv4 routes are advertised by RTR2 to RTR3 over IPv6 peering, the first 32 bits of RTR2's IPv6 address is converted to an IPv4 address. This IPv4 address is advertised as the nexthop address to RTR3. If this address results in a Martian address, then RTR3 will ignore the BGP update message, and will not learn the IPv4 routes.

Configuring an inbound routemap on RTR3 to override the nexthop advertised by RTR2 does not avoid this problem because the BGP update message is ignored.

Workaround: Configure an outbound routemap on RTR2 to explicitly set the IPv4 nexthop rather than allow the protocol to derive it implicitly. (CSCsk65139)

- When you try to modify the allocated link bandwidth for IPv6 EIGRP using the **ipv6 bandwidth-percent eigrp as-number percent** command, the supervisor engine reloads. If you enable redundancy, the STANDBY supervisor engine changes to ACTIVE, and the reloaded supervisor engine is set to STANDBY.

Workaround: None. (CSCso30051)

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running IOS, the standby supervisor engine is in ROMMON mode, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down, but the active supervisor engine does not detect it.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisors with the redundancy reload shelf command.
- Power-cycle the STANDBY supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- The message “**Module M linecard watchdog has expired**” appears when the switch boots. The message may appear when a linecard boots, depending on how the hardware has powered-up.

Workaround: Reset the linecard. (CSCsq21215)

- Changing flow control configuration with traffic and pause frames causes some traffic loss.

This problem can happen when pause frames are sent to the switchport and the flow control receive configuration is toggled on 10G port.

Workaround: Change the flow control receive configuration when no traffic exists. (CSCso71647)

- IGMP snooping entries are active even after you disable IGMP snooping globally.

Workaround: Disable IGMP snooping on all the relevant VLANs before disabling it globally. (CSCsq71546)

- On a Catalyst 4500 series switch running Cisco IOS Release 12.2(47)SG, if you configure the switch port connecting to the AAA server as a Layer 2 interface with SVI enabled on the access VLAN, any MDA (Multi-domain Authentication) port configured with port security and spanning-tree portfast might experience an 802.1X security violation when an 802.1X enabled phone tries to authenticate on the MDA port.

Workarounds:

- a. Disable port security on the port, or connect the switch to the AAA server through a standard Layer 3 port.
- b. Disable spanning-tree portfast.

(CSCsq62342)

- Percentage based input policer on an interface with non-default speed doesn't work after the system reloads.

Workaround: Remove and re-apply the service-policy on the interface.

(CSCsq79073)

- When a packet is switched through software on the switch, you might see that the input QoS marking action on that packet does not take effect.

The issue is observed only for packets that are logically switched through the switch but are internally controlled such that on egress the system generated by the switch itself. This can happen for certain snooping features like DAI, IGMP snooping, DHCP snooping, and MLD snooping. This can also happen for IPv4/v6 packets with IP options/ extension headers that need processing in software.

Workaround: None.

(CSCso96660)

- When policer or shape values are specified as a per cent of link bandwidth on a policy and the interface on which they are attached is forced to a specific speed using the **speed 10/100/1000** command, the applied policer or shape value might correspond to the new forced speed.

Example:

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Use either the **speed auto 10/100/1000** command or the absolute policer or shape values instead of percentage values.

Example:

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- Channel unbundles and re-bundles when a policy map with per cent based actions is shared between channel member ports and another standalone port, and the standalone port is modified from Layer 2 to Layer 3 or Layer 3 to Layer 2.

Workaround: None. (CSCso54096)

- In SSO mode, when you add, remove, or modify service-policies to port-channel members, you see the following traceback on both the active and standby supervisor engine:

```
03:50:00: %SM-4-BADEVENT: STANDBY:Event 'bundle_sync' is invalid for the current state
'COLLECTING_DISTRIBUTING': lacp_mux Gi7/7 - mux
-Traceback= 10B97B80 10B98294 10189F78 1038FE0C 103944FC 1055E420 1055C4B8 10A2C28C
10A2AE88 10A2A4B0 10A27A18 10A225E8 1059E824 10595AAC
```

Workaround: None. CSCso23786)

- IPv6 MLD entries are active even if an IPv6 MLD related configuration does not exist.

Workaround: Unconfigure all generic QOS policies from the system. (CSCsq84853)

- IPv6 entries are active in the CAM; the CPU receives IPv6 packets.

Workaround: Unconfigure any generic QOS policies from the system. The QoS policies with the **match any** attribute cause IPv6 entries to become active. If the switch is a pure Layer 2 device, remove the generic protocol family attributes and narrow it to the protocol family.

(CSCsq84796)

- Initially, REP configured with VLAN Load Balancing (VLB) works correctly. When you enter a force-switchover on the switch, that has a port acting as the secondary ALT port, a loop is induced in the topology.

Workaround: Enter shut, then no-shut on any REP port (of the same segment in which VLB is configured) in the topology. (CSCsq75342)

- In Cisco IOS Release 12.2(46)SG, if flexlink is applied to a pair of etherchannels, then flexlink config may not be applied after a reboot, if the backup EtherChannel is defined after the flexlink configuration.

Workaround: Define the backup etherchannel before applying the flexlink command.
(CSCsq13477)

- In Cisco IOS Release 12.2(46)SG, if an etherchannel is a member of a flexlink pair, then static MAC addresses configured on the EtherChannel are not moved to the alternate port when the EtherChannel fails (flexlink failure)

Workaround: None. (CSCsq99468)

- Performing a default interface operation on an interface with auto-QoS enabled results in an error message and the loss of the auto-QoS configuration. For example, the following sequence of operation results in a loss of the configuration:

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

Workaround: Replace the **default interface** command with the following:

```
config# interface interface-number
config-if# switchport
```

(CSCsq47116)

- The IPv6 ICMP neighbor state changes from **REACH** to **STALE** after 15 secs of inactivity on the link.

Workaround: Ping the global and link local addresses of the neighbor to ascertain and reinstate reachability. (CSCsq77181)

- IPv6 EIGRP routes are not learned through the port channel.

Workaround: Unconfigure the port channel and the associated physical port, and reconfigure them.
(CSCsq74229)

- When a CFM Inward Facing MEP(IFM) is configured on a VLAN that is not allocated on a switch port that is DOWN, the **show ethernet cfm maintenance-points local** command displays the IFM CC Status as **Inactive**. Then, you allocate the VLAN, the CC-status remains **Inactive**.

You only see this symptom if you did not allocate a VLAN before you configure the IFM, then at a later time allocate the same VLAN.

Workaround: Unconfigure, then reconfigure the IFM on the port.

- With CFM, if the VLAN associated with the service instance/MEP is allocated after the Inward Facing MEP (IFM) is configured on an interface whose status is **down**, the IFM CC status remains **inactive** in the output of the **show ethernet CFM maintenance local** command. Also, the CFM remote neighbor is not seen.

This behavior is only seen when VLAN is allocated after the IFM is configured.

Workaround: Unconfigure with the **no ethernet cfm mep level mpid vlan** command, then reconfigure the IFM with the **ethernet cfm mep level mpid vlan** command on the port after the VLAN is allocated. Verify that the C-Status of the IFM is Active with the **show ethernet cfm maintenance-points local** command. (CSCsm85460)

- When you use a Catalyst 4500 series switch with Supervisor Engine 6-E with an output service policy configured on an interface, you observe output drops due to a queue full condition when you enter shut/no shut on a different interface that also has the same output service policy applied.

This issue is open in Cisco IOS Releases 12.2(40)SG, 12.2(44)SG and 12.2(46)SG.

This issue is resolved in 12.2(50)SG.

Workaround: Do not use the qos autoqos macro.

When a policy-map is shared on more than one target, it should not use any percentage based actions; police, shape, and bandwidth actions must use absolute values. This requires a different policy-map for each of the four interface speeds supported on the switch - 10M, 100M, 1G, and 10G. So, rather than having a single policy-map as enabled through percentage-based actions, you must create four distinct policy-maps. This applies to all shared policy-maps, independent of direction of service-policy.

(CSCsr12142)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(46)SG

This section lists the resolved caveats in Release 12.2(46)SG:

- After entering the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs appear on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF
```

```
00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

At this point, if you revert to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

Workaround: First enter the **no bgp dampening** command, and then enter the **bgp dampening** command. (CSCse12485)

- The REP Admin VLAN and RSPAN destination VLAN should not match. A given VLAN can be configured as a REP Admin VLAN as well as an RSPAN destination VLAN.

Workaround: Ensure that the REP Admin VLAN and the RSPAN destination VLAN differ. (CSCso12495)

- If VLAN load balancing is active, the failure of a segment or the removal of supervisor engine may cause looping in the REP segment.

Workaround: None. (CSCsm61748)

- Not all combinations of features can be simultaneously supported by the hardware. When an supportable combination is configured, packets are processed in software and a log message is generated:

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

One feature combination that can trigger this problem is a QoS policy that matches on the cos bits with an IPv6 ACL configuration, which in turn matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets ranging from /81 to /127 also trigger this behavior if IPv6 multicast routing is enabled.)

Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, design the IPv6 network using /80 subnets or larger. (CSCsk79791)

- The **ip icmp unreachable** command may affect ICMP unreachable generation for both IPv4 and IPv6 packets received on the Layer 3 interface. Furthermore, a Layer 3 deny ACL on a Layer 3 interface with an IPv6 address may not copy the denied traffic to the CPU, bypassing ICMP unreachable generation.

The first problem occurs on a dual Layer 3 interface where both IPv4 and IPv6 addresses are configured. The second problem occurs when all Layer 3 interfaces in a switch are configured with the IPv6 address only.

Workarounds: Avoid using a dual Layer 3 interface with both IPv6 and IPv4 addresses configured.

Avoid using a switch as a purely IPv6 Layer 3 interface-only router. Ensure that it has at least one Layer 3 interface per SVI with an IPv4 address configured. (CSCsk77234)

- When you toggle an interface configuration from a Layer 3/router port to a Layer 2/switch port and then to a Layer 3/router port, an IPv6 ACL attached on the original router interface may not get removed properly in the TCAM hardware even though the router interface's IOS configuration is unconfigured.

Workaround: Before switching a Layer 3 interface from a router port to a switch port, unconfigure the IPv6 ACL on the router interface. This ensures that the IPv6 ACL is cleaned up properly both in the IOS running configuration as well as in the TCAM hardware. (CSCsk60775)

- The LEDs on E-series supervisor and linecards remain green even when the module reports a critical or shutdown temperature alarm. The LEDs should turn orange or red.

This occurs on all E-series linecards that report critical or shutdown temperature alarms. The actual temperatures and the alarm states are visible in the output of the **show environment temperature** command.

Workarounds: None for LED colors. However, when an alarm is raised or cleared, console log messages and SNMP traps are entered. Also, the current status of any temperature alarms are visible in the output of the **show environment temperature** command. (CSCsk57143)

- When a non-default duplex setting is applied to a FastEthernet interface and you upgrade from Cisco IOS Release 12.2(31)SGA to 12.2(40)SG, the duplex settings on FastEthernet settings are lost. The interface reverts to its default duplex setting, and the duplex setting no longer appears in the output of the **show running** command.

Workaround: If non-default duplex settings are in the running configuration, note them prior to upgrading, and reapply them after the upgrade completes. (CSCsk83670)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is not applied on reload.

Workaround: Reapply the policy-map. (CSCsk75793)

- A port can be either a member of a port channel or be applied with auto-QoS, but not both. The two are mutually exclusive features.

Currently, if auto-QoS is applied to a port that is already a member of a port channel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a port channel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a port channel. (CSCsi95018)

- If *exceed burst* is not explicitly configured for a dual-rate policer, the **show policy-map** command displays 0 as the burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *exceed burst* value programmed. (CSCsj44237)

- On switches with redundant WS-X45-SUP6-E supervisor engines and WS-X4506-GB-T interfaces that have been configured to use RJ-45, the QoS configuration on the interface is ineffective after a SSO switchover. Furthermore, you may lose the QoS configuration if the media type is changed to SFP and then back to RJ-45.

The QoS configuration is present in the running configuration but is not honored on the interface.

Workaround: Reapply the QoS configuration to the interface. (CSCsm58839)

- If you configure IPv6 MTU on an interface using the **ipv6 mtu mtu-value** command without first enabling IPv6 on the interface, your switch might pause indefinitely on startup.

Workarounds: Before configuring IPv6 MTU on an interface, you must enable IPv6 on the interface. To enable IPv6, use the **ipv6 enable** command.

If you encounter this problem, use the following commands to recover your switch:

- At the ROMMON prompt, enter the **confreg** command to ignore the startup configuration.
- Enter the **reset** command to reboot your switch.
- Enter the **copy startup-config running-config** command to copy your startup configuration to your running configuration

4. Enter the **ipv6 enable** command to enable IPv6 on the interfaces.
5. Enter the **ipv6 mtu *mtu-value*** command to configure IPv6 MTU on your interface.
6. Enter the **copy running-config startup-config** command to save your recovered configuration.
7. Enter the **reload** command on the switch to return to ROMMON.
8. From ROMMON, enter the **confreg** command to process the startup config.
9. Reset the switch to resume normal operation. (CSCso42867)

- A switch directly connected to the uplink ports on a Catalyst 4500 supervisor engine does not see link down when the engine reloads. So, if UDLD is enabled, a link partner will enter the err-disable state.

Workaround: Shut down supervisor uplink ports prior to reload. (CSCsl34390)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

Open Caveats in Cisco IOS Release 12.2(44)SG1

This section lists the open caveats in Cisco IOS Release 12.2(44)SG1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# show policy-map int
FastEthernet3/2

Service-policy output: p1
```

```

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnac121
police: Per-interface
Conform: 9426560 bytes Exceed: 16573440 bytes

```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- This is also seen if the switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF
```

```
00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCSi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCSi60898)

- If an Cisco IP Phone is attached to a supplicant, when you reload a DUT port configured with MDA and attached to the phones and supplicants, the port will not pass traffic. Phone will enter an unknown state.

This problem is not observed if the phone is a stand alone device.

Workarounds: Powercycle the Cisco IP phone. (CSCsk81297)

- After a data device is authorized (thru dot1x or MAB) on a port configured with Multi-Domain Authentication (MDA), changing the access VLAN causes traffic loss for this device even if no device is connected on the port. It does *not* affect the traffic from the voice device connected to the port.

Workaround: Enter the **shutdown**, then **no shutdown** commands on the interface after changing the access VLAN on the port. (CSCsk45969)

- The REP Admin VLAN and RSPAN destination VLAN should not match. A given VLAN can be configured as a REP Admin VLAN as well as an RSPAN destination VLAN.

Workaround: Ensure that the REP Admin VLAN and the RSPAN destination VLAN differ. (CSCso12495)

- When traffic is sent on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225ms.

Workaround: None. (CSCsm30320)

- In REP, when you change the VLAN Load Balancing configuration to reflect different VLAN blocking, Manual Preemption doesn't occur.

Workaround: Intentionally fail the link between two switches by physically pulling the cable or shutting down the interface. Then, return the links to a normal condition. This is followed by delayed preemption, which you might have already configured. (CSCsm91997)

- Under VLAN Load Balancing, the failure of a segment or the removal of supervisor engine may cause looping in the REP segment.

Workaround: None. (CSCsm61748)

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workarounds: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets is processed in software and a log message indicating this is generated:

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)

Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or bandwidth value might correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- The **ip icmp unreachable** command may affect ICMP unreachable generation for both IPv4 and IPv6 packets received on the Layer 3 interface. Furthermore, a Layer 3 deny ACL on a Layer 3 interface with an IPv6 address may not copy the denied traffic to the CPU, bypassing ICMP unreachable generation.

The first problem occurs on a dual Layer 3 interface where both IPv4 and IPv6 address are configured. The second problem occurs when all Layer 3 interfaces in a switch are configured with IPv6 address only.

Workarounds: Avoid using a dual Layer 3 interface with both IPv6 and IPv4 address configured.

Avoid using a switch as a purely IPv6 Layer 3 interface-only router. Ensure that it has at least one Layer 3 interface per SVI with IPv4 address configured. (CSCsk77234)

- When you toggles an interface configuration from Layer 3/router port to Layer 2/switch port, and back to Layer 3/router port, an IPv6 ACL attached on the original router interface may not get flushed properly in the TCAM hardware even though the router interface's IOS configuration is unconfigured.

Workaround: Before switching a Layer 3 interface from a router port to a switch port, unconfigure the IPv6 ACL on the router interface. This will ensure that the IPv6 ACL is cleaned up properly both in the IOS running configuration as well as in the TCAM hardware. (CSCsk60775)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGalInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- The LEDs on E-series supervisor and line cards remain green even when the module reports a critical or shutdown temperature alarm. The LEDs should turn orange or red.

This occurs on all E-series line cards that report critical or shutdown temperature alarms. The actual temperatures and the alarm states are visible in the output of **show environment temperature** command.

Workarounds: None for LED colors. However, when an alarm is raised or cleared, console log messages and SNMP traps are entered. Also, the current status of any temperature alarms are visible in the output of the **show environment temperature** command. (CSCsk57143)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- When a non-default duplex setting is applied to a FastEthernet interface and you upgrade from Cisco IOS Release 12.2(31)SGA to 12.2(40)SG, the duplex settings on FastEthernet settings are lost. The interface reverts to its default duplex setting, and the duplex setting no longer appears in the output of the **show running** command.

Workaround: If non-default duplex settings are in the running config, note them prior to upgrading, and reapply them after the upgrade completes. (CSCsk83670)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. CSCsk67395)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is not applied on reload.

Workaround: Re-apply the policy-map. (CSCsk75793

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- A port can be either a member of a portchannel or have auto-QoS applied to it, but not both. The two are mutually exclusive features.

Currently, if auto-QoS is applied to a port that is already a member of a portchannel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a portchannel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a portchannel. (CSCsi95018)

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays "0" as the burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *exceed burst* value programmed. (CSCsj44237)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map command** displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- Executing **default interface** twice on a port configured with the cisco-phone macro displays the back trace.

Workaround: Remove the configuration line by line without entering the **default interface** command. (CSCsj23103)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- If you configure a QoS policy with queuing actions (like sharing and shaping) on WS-X4648-RJ45V-E (PoE) and WS-X4648-RJ45V+E (Premium PoE with 30 W per port) line cards, the sharing and shaping percentage error increases to 3 per cent after a SSO switch over.

Workaround: Do one of the following:

- Remove the service-policy from the interface and reapply the configuration through the command **[no] service-policy {input/output}**.
- Enter the **shutdown** and **noshutdown** commands.

(CSCsm45156)

- On switches with redundant WS-X45-SUP6-E supervisor engines and WS-X4506-GB-T interfaces that have been configured to use RJ-45, the QoS configuration on the interface is ineffective after a SSO switchover. Furthermore, you may lose the QoS configuration if the media type is changed to SFP and then back to RJ-45.

The QoS configuration is present in the running configuration but is not honored on the interface.

Workaround: Reapply the QoS configuration to the interface. (CSCsm58839)

- When you specify a DBL action for the 'class-default' class-map in a policy-map, it might not work depending on the size of the default queue.

Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. The size range is dictated by the **queue-limit** command. (CSCso06422)

- When IPv4 routes are advertised by RTR2 to RTR3 over IPv6 peering, the first 32 bits of RTR2's IPv6 address is converted to an IPv4 address. This IPv4 address is advertised as the nexthop address to RTR3. If this address results in a Martian address, then RTR3 will ignore the BGP update message, and will not learn the IPv4 routes.

Configuring an inbound routemap on RTR3 to override the nexthop advertised by RTR2 does not avoid this problem because the BGP update message is ignored.

Workaround: Configure an outbound routemap on RTR2 to explicitly set the IPv4 nexthop rather than allow the protocol to derive it implicitly. (CSCsk65139)

- When we try to modify the allocated link bandwidth for IPv6 EIGRP using the **ipv6 bandwidth-percent eigrp as-number percent** command, the supervisor engine reloads. If you enable redundancy, the STANDBY supervisor engine changes to ACTIVE, and the reloaded supervisor engine is set to STANDBY.

Workaround: None. (CSCso30051)

- Uplinks go down when upgrading the rommon of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the ACTIVE supervisor engine is running IOS, the STANDBY supervisor engine is in rommon, and the STANDBY's rommon is upgraded from version 0.34 or to a later version. The upgrade process will cause the uplinks on the STANDBY supervisor engine to go down but the ACTIVE supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisors with the redundancy reload shelf command.
- Power-cycle the STANDBY supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- If you configure IPv6 MTU on an interface using the **ipv6 mtu mtu-value** command without first enabling IPv6 on the interface, your switch might pause indefinitely on startup.

Workarounds: Before configuring IPv6 MTU on an interface you must enable IPv6 on the interface. To enable IPv6, use the **ipv6 enable** command.

If you encounter this, enter the following commands in this order to recover your switch:

10. from the rommon prompt, use the **confreg** command to ignore the startup configuration
11. **reset** command to reboot your switch
12. **copy startup-config running-config** command to copy your startup configuration to your running configuration
13. **ipv6 enable** command to enable IPv6 on the interfaces
14. **ipv6 mtu mtu-value** command to configure IPv6 MTU on your interface
15. **copy running-config startup-config** command to save your recovered configuration
16. **reload** command on the switch to return to Rommon
17. from rommon, use the **confreg** command to process the startup config
18. reset the switch to resume normal operation . (CSCso42867)

- When you use a Catalyst 4500 series switch with Supervisor Engine 6-E with an output service policy configured on an interface, you observe output drops due to a queue full condition when you enter shut/no shut on a different interface that also has the same output service policy applied.

This issue is open in Cisco IOS Releases 12.2(40)SG, 12.2(44)SG and 12.2(46)SG.

This issue is resolved in 12.2(50)SG.

Workaround: Do not use the qos autoqos macro.

When a policy-map is shared on more than one target, it should not use any percentage based actions; police, shape, and bandwidth actions must use absolute values. This requires a different policy-map for each of the four interface speeds supported on the switch - 10M, 100M, 1G, and 10G.

So, rather than having a single policy-map as enabled through percentage-based actions, you must create four distinct policy-maps. This applies to all shared policy-maps, independent of direction of service-policy.

(CSCsr12142)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(44)SG1

This section lists the resolved caveats in Release 12.2(44)SG1:

- When an interface configured as an EIGRP passive interface experiences a link up or link down event, the switch may have an unexpected reload. This is usually accompanied with the message: "Vector 300" message on the console."

Workaround: Remove the EIGRP passive interface configuration.

Upgrading to Cisco IOS Release 12.2(44)SG1 or 12.2(46)SG for all supervisors eliminates the problem.

This defect is not present in the 12.2(31)SGA software train, which only supports classic supervisors. (CSCsk04287).

- On Catalyst 4500 series switch with dual 4200W AC power supplies with one or both 220V connections, you might observe the following messages:

```
Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the
chassis are receiving different voltage inputs
```

```
Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the
chassis are of different types (AC/DC) or wattage
```

On ports with PoE devices connected, you might also see:

```
%ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi2/33: inline power denied
```

The affected power supply experiences a temporary shut down and power supply redundancy is lost. Power for data and chassis is decremented and occasionally the linecard(s) shut down. Also, power for PoE will decrement, causing PDs to shut down and reset.



Note If both the units have 110V inputs, they are not affected. (the output current is lower with both 110V input connections, see Power Supply Calculator on CCO, <http://tools.cisco.com/cpc/launch.jsp>.)

Workaround: None. (CSCso67729)

Open Caveats in Cisco IOS Release 12.2(44)SG

This section lists the open caveats in Cisco IOS Release 12.2(44)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# show policy-map int
FastEthernet3/2

Service-policy output: p1

Class-map: c1 (match-all)
 0 packets-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- This is also seen if the switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF
```

```
00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

- If an Cisco IP Phone has an supplicant attached, upon reloading a DUT port configured with MDA and attached to phones and supplicants, the port will not pass traffic. Phone will in an unknown state. Problem is not observed if the phone is a stand alone device.

Workarounds: Powercycle the Cisco IP phone. (CSCsk81297)

- After a data device is authorized (thru dot1x or MAB) on a port configured with Multi-Domain Authentication (MDA), changing the access VLAN causes traffic loss for this device even if no device is connected on the port. It does *not* affect the traffic from the voice device connected to the port.

Workaround: Enter the **shutdown** and **no shutdown** commands on the interface after changing the access VLAN on the port. (CSCsk45969)

- The REP Admin VLAN and RSPAN destination VLAN should not match. A given VLAN can be configured as a REP Admin VLAN as well as an RSPAN destination VLAN.

Workaround: Ensure that the REP Admin VLAN and the RSPAN destination VLAN differ. (CSCso12495)

- When traffic is sent on a VLAN ID higher than 3000, the convergence timing caused by a failure exceeds 225ms.

Workaround: None. (CSCsm30320)

- In REP, when you change the VLAN Load Balancing configuration to reflect different VLAN blocking, Manual Preemption doesn't occur.

Workaround: Intentionally fail the link between two switches by physically pulling the cable or shutting down the interface. Then, return the links to a normal condition . This is followed by delayed preemption, which you might have already configured. (CSCsm91997)

- Under VLAN Load Balancing, the failure of a segment or the removal of supervisor engine may cause looping in the REP segment.

Workaround: None. (CSCsm61748)

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workarounds: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets is processed in software and a log message indicating this is generated:

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)

Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or bandwidth value might correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- The **ip icmp unreachable** command may affect ICMP unreachable generation for both IPv4 and IPv6 packets received on the Layer 3 interface. Furthermore, a Layer 3 deny ACL on a Layer 3 interface with an IPv6 address may not copy the denied traffic to the CPU, bypassing ICMP unreachable generation.

The first problem occurs on a dual Layer 3 interface where both IPv4 and IPv6 address are configured. The second problem occurs when all Layer 3 interfaces in a switch are configured with IPv6 address only.

Workarounds: Avoid using a dual Layer 3 interface with both IPv6 and IPv4 address configured.

Avoid using a switch as a purely IPv6 Layer 3 interface-only router. Ensure that it has at least one Layer 3 interface per SVI with IPv4 address configured. (CSCsk77234)

- When you toggles an interface configuration from Layer 3/router port to Layer 2/switch port, and back to Layer 3/router port, an IPv6 ACL attached on the original router interface may not get flushed properly in the TCAM hardware even though the router interface's IOS configuration is unconfigured.

Workaround: Before switching a Layer 3 interface from a router port to a switch port, unconfigure the IPv6 ACL on the router interface. This will ensure that the IPv6 ACL is cleaned up properly both in the IOS running configuration as well as in the TCAM hardware. (CSCsk60775)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGallInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- The LEDs on E-series supervisor and line cards remain green even when the module reports a critical or shutdown temperature alarm. The LEDs should turn orange or red.

This occurs on all E-series line cards that report critical or shutdown temperature alarms. The actual temperatures and the alarm states are visible in the output of **show environment temperature** command.

Workarounds: None for LED colors. However, when an alarm is raised or cleared, console log messages and SNMP traps are entered. Also, the current status of any temperature alarms are visible in the output of the **show environment temperature** command. (CSCsk57143)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- When a non-default duplex setting is applied to a FastEthernet interface and you upgrade from Cisco IOS Release 12.2(31)SGA to 12.2(40)SG, the duplex settings on FastEthernet settings are lost. The interface reverts to its default duplex setting, and the duplex setting no longer appears in the output of the **show running** command.

Workaround: If non-default duplex settings are in the running config, note them prior to upgrading, and reapply them after the upgrade completes. (CSCsk83670)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. (CSCsk67395)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is not applied on reload.

Workaround: Re-apply the policy-map. (CSCsk75793)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- A port can be either a member of a portchannel or have auto-QoS applied to it, but not both. The two are mutually exclusive features.

Currently, if auto-QoS is applied to a port that is already a member of a portchannel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a portchannel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a portchannel. (CSCsi95018)

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays "0" as the burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *exceed burst* value programmed. (CSCsj44237)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map command** displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command to find the actual *burst* value programmed. (CSCsi71036)

- Executing **default interface** twice on a port configured with the cisco-phone macro displays the back trace.
Workaround: Remove the configuration line by line without entering the **default interface** command. (CSCsj23103)
- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.
Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.
Workaround: None. (CSCsl72868)
- If you configure a QoS policy with queuing actions (like sharing and shaping) on WS-X4648-RJ45V-E (PoE) and WS-X4648-RJ45V+E (Premium PoE with 30 W per port) line cards, the sharing and shaping percentage error increases to 3 per cent after a SSO switch over.
Workaround: Do one of the following:
 - Remove the service-policy from the interface and reapply the configuration through the command **[no] service-policy {input/output}**.
 - Enter **shutdown** then **noshutdown**.
 (CSCsm45156)
- On switches with redundant WS-X45-SUP6-E supervisor engines and WS-X4506-GB-T interfaces that have been configured to use RJ-45, the QoS configuration on the interface is ineffective after a SSO switchover. Furthermore, you may lose the QoS configuration if the media type is changed to SFP and then back to RJ-45.
The QoS configuration is present in the running configuration but is not honored on the interface.
Workaround: Reapply the QoS configuration to the interface. (CSCsm58839)
- When you specify a DBL action for the 'class-default' class-map in a policy-map, it might not work depending on the size of the default queue.
Workaround: To ensure that the DBL action operates on the default queue, use the **queue-limit** command to specify an explicit queue size. The size range is dictated by the **queue-limit** command. (CSCso06422)
- When IPv4 routes are advertised by RTR2 to RTR3 over IPv6 peering, the first 32 bits of RTR2's IPv6 address is converted to an IPv4 address. This IPv4 address is advertised as the nexthop address to RTR3. If this address results in a Martian address, then RTR3 will ignore the BGP update message, and will not learn the IPv4 routes.
Configuring an inbound routemap on RTR3 to override the nexthop advertised by RTR2 does not avoid this problem because the BGP update message is ignored.
Workaround: Configure an outbound routemap on RTR2 to explicitly set the IPv4 nexthop rather than allow the protocol to derive it implicitly. (CSCsk65139)
- When we try to modify the allocated link bandwidth for IPv6 EIGRP using the **ipv6 bandwidth-percent eigrp as-number percent** command, the supervisor engine reloads. If you enable redundancy, the STANDBY supervisor engine changes to ACTIVE, and the reloaded supervisor engine is set to STANDBY.
Workaround: None. (CSCso30051)

- Uplinks go down when upgrading the rommon of an WS-X45-SUP6-E supervisor from version 0.34 to a later version.

This behavior occurs in a redundant switch when the ACTIVE supervisor engine is running IOS, the STANDBY supervisor engine is in rommon, and the STANDBY's rommon is upgraded from version 0.34 or to a later version. The upgrade process will cause the uplinks on the STANDBY supervisor engine to go down but the ACTIVE supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisors with the redundancy reload shelf command.
- Power-cycle the STANDBY supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. (CSCsm81875)

- If you configure IPv6 MTU on an interface using the `ipv6 mtu mtu-value` command without first enabling IPv6 on the interface, your switch might pause indefinitely on startup.

Workarounds: Before configuring IPv6 MTU on an interface you must enable IPv6 on the interface. To enable IPv6, use the `ipv6 enable` command.

If you encounter this enter the following commands to recover your switch:

-
19. from the rommon prompt, use the **confreg** command to ignore the startup configuration
 20. **reset** command to reboot your switch
 21. **copy startup-config running-config** command to copy your startup configuration to your running configuration
 22. **ipv6 enable** command to enable IPv6 on the interfaces
 23. **ipv6 mtu mtu-value** command to configure IPv6 MTU on your interface
 24. **copy running-config startup-config** command to save your recovered configuration
 25. **reload** command on the switch to return to Rommon
 26. from rommon, use the **confreg** command to process the startup config
 27. reset the switch to resume normal operation . (CSCso42867)
-

- When you use a Catalyst 4500 series switch with Supervisor Engine 6-E with an output service policy configured on an interface, you observe output drops due to a queue full condition when you enter shut/no shut on a different interface that also has the same output service policy applied.

This issue is open in Cisco IOS Releases 12.2(40)SG, 12.2(44)SG and 12.2(46)SG.

This issue is resolved in 12.2(50)SG.

Workaround: Do not use the qos autoqos macro.

When a policy-map is shared on more than one target, it should not use any percentage based actions; police, shape, and bandwidth actions must use absolute values. This requires a different policy-map for each of the four interface speeds supported on the switch - 10M, 100M, 1G, and 10G. So, rather than having a single policy-map as enabled through percentage-based actions, you must create four distinct policy-maps. This applies to all shared policy-maps, independent of direction of service-policy.

(CSCsr12142)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(44)SG

This section lists the resolved caveats in Release 12.2(44)SG:

- When a service-policy is removed from a physical port that is member of an ether channel, a LACP or PAGP protocol-based ether channel goes down. The port-channel members get bundled back in but remain in *suspended* state due to failure to exchange the protocol packets with the other end.

Workarounds: Before removing the service policy from a ether channel member, remove it from the channel. Then, return it to the channel. (CSCsk70568)

- When using *bandwidth percentage* actions in a queuing policy-map, the actual bandwidth share differs from that of the configured policy-map.

In a queuing QoS policy, there can be zero or more queuing classes that have an explicit, user specified, bandwidth share specified. There can be zero or more queuing classes that do not have such user specified bandwidth share. The system takes the unallocated bandwidth share and allocates it equally among the latter set of classes.

When using percentage-based bandwidth allocation, if the share comes to less than 1%, the queues corresponding to those classes do not get updated in hardware with the new bandwidth share. These queues get more than the expected share of bandwidth.

Workarounds: Ensure that the unallocated bandwidth percentage is at least equal to the number of queues that do not have the explicit **bandwidth percentage** command. This should include the default as well as priority queues. (CSCsk77757)

- When a service policy on a port-channel member port is modified, traffic may be dropped for some of the classes.

Workaround: Do the following:

- a. Un-configure the interface(s) on which this policy-map is attached from the portchannel.
- b. Modify the policy-map.

c. Configure the interface(s) in the portchannel.

- If you configure auto-QoS on a Layer 2 port, change the port to Layer 3, and then remove auto-QoS on the port, the process will not cleanup the QoS service policies on the port due to inconsistency between when auto-QoS was applied versus when it was removed.

Similarly, if you Configure auto-QoS on a Layer 3 port, change the port to Layer 2, and then remove auto-QoS on the port, the process does not cleanly remove QoS service policies on the port.

A sequence similar to the following would lead to the problem on port g2/1

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
no auto qos voice trust
```

Workaround: Revert the port setting to the setting when auto-QoS was applied. If auto-QoS was enabled when the port was a Layer 2 port, it should be reverted to Layer 2 before auto-QoS is removed. Similarly, if the port was set to Layer 3 when auto-QoS was initially applied, it must be reverted to Layer 3 before auto-QoS is removed.

Referring to the problem sequence, first apply auto-QoS to a Layer 2 port, change it to layer 3, then revert to Layer 2 and remove auto-QoS:

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
switchport
no auto qos voice trust
```

(CSCsk95871)

- When a queuing policy is attached to a trunk port configured with a per-port per-VLAN QoS policy, the port-level queuing policy is processed as part of a per-VLAN policy and is rejected on bootup.

Queuing policy is supported on a physical interface in the output direction only.

Workaround: After bootup, reattach a queuing policy on a physical interface. (CSCsk87548)

- When you delete a port-channel with a per-port per-VLAN QoS policy, the switch crashes.

Workaround: Before deleting the port-channel, do the following:

1. Remove any per-port per-VLAN QoS policies, if any.
2. Remove the VLAN configuration on the port-channel with the **no vlan-range** command.

(CSCsk91916)

- The cbQosPoliceCfgTable mib object is *not* populated by the **police bps byte** command.

Workaround: None. (CSCsk45940)

- If a class-map is configured with **exceed-action drop**, re-configuring the same class-map with **exceed-action transmit** causes class-map configurations to conflict for the same class-map.

Workaround: If you plan to change a class-map action, such as **exceed-action**, you need to remove the class-map with the **no class c1** command under policy-map submenu. Then, apply the new class-map with the updated changes.

CSCsk70826)

- A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl>
(CSCsj85065)

- Cisco IOS Software Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi>
(CSCsk93241)

Open Caveats in Cisco IOS Release 12.2(40)SG

This section lists the open caveats in Cisco IOS Release 12.2(40)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:


```
clearwater# show policy-map int
FastEthernet3/2

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets<-----It stays at '0' despite of traffic being received
Match: access-group name fnacl21
police: Per-interface
  Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned. (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
 - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
 - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rpf-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

This could occur for these reasons:

- A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
- This is also seen if the switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)
- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF
```

```
00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

Workaround: None. (CSCsg58526)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

This does not affect performance.

Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

Workaround: None. This is an informational message. (CSCsi60898)

Supervisor Engine 6-E Specific

- Software qos does not match a .1Q packet properly for applying the desired qos actions.

Workarounds: None.

The support to handle .1Q packets for software QoS lookup unavailable in the Cisco IOS Release 12.2(40)SG release. (CSCsk66449)

- When a service-policy is removed from a physical port that is member of an ether channel, a LACP or PAGP protocol-based ether channel goes down. The port-channel members get bundled back in but remain in *suspended* state due to failure to exchange the protocol packets with the other end.

Workarounds: Before removing the service policy from a ether channel member, remove it from the channel. Then, return it to the channel. (CSCsk70568)

- When using *bandwidth percentage* actions in a queuing policy-map, the actual bandwidth share differs from that of the configured policy-map.

In a queuing QoS policy, there can be zero or more queuing classes that have an explicit, user specified, bandwidth share specified. There can be zero or more queuing classes that do not have such user specified bandwidth share. The system takes the unallocated bandwidth share and allocates it equally among the latter set of classes.

When using percentage-based bandwidth allocation, if the share comes to less than 1%, the queues corresponding to those classes do not get updated in hardware with the new bandwidth share. These queues get more than the expected share of bandwidth.

Workarounds: Ensure that the unallocated bandwidth percentage is at least equal to the number of queues that do not have the explicit **bandwidth percentage** command. This should include the default as well as priority queues. (CSCsk77757)

- Not all combinations of features can be simultaneously supported by the hardware. When such a feature combination is configured, packets is processed in software and a log message indicating this is generated:

```
%C4K_HWACLMAN-4-ACLHWLABLELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

One feature combination that can trigger this problem is the attempt to combine a QoS policy that matches on cos bits with IPv6 ACL configuration that matches on IPv6 source addresses that partially mask in the lower 48 bits of the address. (IPv6 subnets in the /81 to /127 range will also trigger this behavior if IPv6 multicast routing is enabled.)

Workaround: Do not configure feature combinations that conflict. Currently the above conflict between QoS policies matching on COS bits and IPv6 configuration with partial masking of the lower 48 bits of the source address is the only known conflicting feature combination. If matching on COS bits is required by the QoS policy, architect the IPv6 network using /80 subnets or larger. (CSCsk79791)

- When policer or shape or shape values are specified in terms of percentage of link bandwidth on a policy and the interface on which it is attached is forced to a specific speed with the **speed 10/100/1000** command, the applied policer or shape or shape value might correspond to the new forced speed.

Service policy has to be configured with percentage police or shape or share values and the link speed is forced to a specific values. For example

```
Policy-map p1
  class-map c1
    police rate percent 10
```

Workaround: Either use the **speed auto 10/100/1000** command or the absolute policer, shape or shape values rather than percentage values. For example,

```
Policy-map p1
  class-map c1
    police rate 10 mbps
```

(CSCsk56877)

- The **ip icmp unreachable** command may affect ICMP unreachable generation for both IPv4 and IPv6 packets received on the Layer 3 interface. Furthermore, a Layer 3 deny ACL on a Layer 3 interface with an IPv6 address may not copy the denied traffic to the CPU, bypassing ICMP unreachable generation.

The first problem occurs on a dual Layer 3 interface where both IPv4 and IPv6 address are configured. The second problem occurs when all Layer 3 interfaces in a switch are configured with IPv6 address only.

Workarounds: Avoid using a dual Layer 3 interface with both IPv6 and IPv4 address configured.

Avoid using a switch as a purely IPv6 Layer 3 interface-only router. Ensure that it has at least one Layer 3 interface per SVI with IPv4 address configured. (CSCsk77234)

- When you toggles an interface configuration from Layer 3/router port to Layer 2/switch port, and back to Layer 3/router port, an IPv6 ACL attached on the original router interface may not get flushed properly in the TCAM hardware even though the router interface's IOS configuration is unconfigured.

Workaround: Before switching a Layer 3 interface from a router port to a switch port, unconfigure the IPv6 ACL on the router interface. This will ensure that the IPv6 ACL is cleaned up properly both in the IOS running configuration as well as in the TCAM hardware. (CSCsk60775)

- Under some conditions, one or more flows continue to be dropped because of DBL even after DBL has been removed from the service-policy.

When an output service-policy is attached to an interface and if the policy is configured to apply DBL on a queue, the flows that are enqueued to the queue are subjected to the DBL algorithm. If one or more flows are classified as *belligerent* (flows do not back-off in response to drops because of congestion in the queue), those flows continue to be classified as belligerent even when DBL is disabled on that queue.

For this condition to persist, the transmit queues in question must remain congested for a long period of time and that congestion must be caused by flows that remain belligerent.

Workaround: Provided the queue in question is non-default (queuing actions are not configured in the class-default class of the policy-map), detach and re-attach the service-policy.

If this happens on the default queue, modifying and resetting some queuing parameters like bandwidth/shape fixes the issue. (CSCsk62457)

- When an E-series switch encounters either a fan tray failure or a supervisor critical temperature, the chassis shuts off. The output of the **show crashdump** command will *not* indicate the cause of the power-down.

Workarounds: Use the **show log** command to determine the cause of the power-down.

- If the log has *LogGalInsufficientFansDetected* messages, the cause was a fan-tray failure.
- If the log has *LogRkiosModuleShutdownTemp* messages, the cause was that the supervisor critical temperature exceeded the failure threshold.

(CSCsk48632)

- The LEDs on E-series supervisor and line cards remain green even when the module reports a critical or shutdown temperature alarm. The LEDs should turn orange or red.

This occurs on all E-series line cards that report critical or shutdown temperature alarms. The actual temperatures and the alarm states are visible in the output of **show environment temperature** command.

Workarounds: None for LED colors. However, when an alarm is raised or cleared, console log messages and SNMP traps are issued. Also, the current status of any temperature alarms are visible in the output of the **show environment temperature** command. (CSCsk57143)

- If a queuing policy-map is detached and attached in quick succession, few packets of non-default class of traffic are dropped.

In this scenario, until the hardware is programmed with a new configuration (**Detach -> Attach**), non-default queues are inactive. So, until these queues are activated, traffic matching these non-default queues is dropped.

Workarounds: None. (CSCsk85379)

- When a service policy on a port-channel member port is modified, traffic may be dropped for some of the classes.

Workaround: Do the following:

- a. Un-configure the interface(s) on which this policy-map is attached from the portchannel.
- b. Modify the policy-map.
- c. Configure the interface(s) in the portchannel.

(CSCsk77119)

- When two switches are connected back-to-back via two or more links and when a packet is locally-originated, the source IP address may not correspond to the IP address of the outgoing interface. A switch receiving such a packet with unicast RPF feature enabled might drop the incoming packet.

Workaround: None. (CSCsh99124)

- A Catalyst 4500 series switch with Supervisor Engine 6-E will support a maximum of 32 MTU values system wide.

On a switch running Cisco IOS Release 12.2(40)SG, all MTU values configured on a line card are set to default when the module is reset. Furthermore, MTU values are not retained for modules that are physically moved.

Workaround: None. (CSCsk52542)

- When a non-default duplex setting is applied to a FastEthernet interface and you upgrade from Cisco IOS Release 12.2(31)SGA to 12.2(40)SG, the duplex settings on FastEthernet settings are lost. The interface reverts to its default duplex setting, and the duplex setting no longer appears in the output of the **show running** command.

Workaround: If non-default duplex settings are in the running config, note them prior to upgrading, and reapply them after the upgrade completes. (CSCsk83670)

- On rare occasions, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you will observe CRC errors after a reload or power cycle when you insert the card or the X2.

Workaround: Reinsert the X2. (CSCsk43618)

- Control plane policing applied to DHCP traffic as identified by the system class-maps system-cpp-dhcp-cs, system-cpp-dhcp-sc, and system-cpp-dhcp-ss may not be effective.

Workaround: None. (CSCsk67395)

- In policy map, if a queuing class with the **bandwidth remaining percent** <> command sits before a priority queuing class configuration, the **bandwidth remaining percent** <> command action is not applied on reload.

Workaround: Re-apply the policy-map. (CSCsk75793)

- When the CPU transmits .1X packet on an interface that has an egress qos policy attached, the packet is not matched and exits without any QoS marking actions.

When a packet is sent to the CPU it may get sent out on some other interface. If so, the original COS value for a .1X packet cannot be matched by software QoS (as per CSCsk66449). The packet is transmitted with whatever COS value it was generated with (7, for the MLDv1 packets described here).

Workaround: None.

Part of the root cause of this problem is captured through CSCsk66449, which indicates that the software QoS cannot match against a .1X packet. (CSCsk72544)

- When the trusted boundary feature is enabled on an interface, there is no command to check the current operating state.

Workaround: None. You cannot explicitly check the trusted boundary state. However, you can indirectly determine this state:

The trusted boundary feature ensures whether the packet's COS/DSCP value will be trusted or not. When the interface is not in a trusted state, the COS/DSCP fields are forced to zero on a received packet.

A QoS policy exists on that interface that uses that COS/DSCP value for classification. Therefore, if the packet classification is based on the packet value, you can infer that the interface is in a trusted state. (CSCsh72408)

- A port can be either a member of a portchannel or have auto-QoS applied to it, but not both. The two are mutually exclusive features.

Currently, if auto-QoS is applied to a port that is already a member of a portchannel, the application is rejected with an error message. However, the reverse is not true. If auto-QoS is applied first and then the port joins a portchannel, the command is accepted.

The following example using port g2/1 shows the type of usage that should be avoided:

```
conf t
int g2/1
```

```
auto qos voice trust
channel-group 10 mode auto
```

This example applies auto-QoS on a port (g2/1) and subsequently makes the port a member of portchannel (10).

Workaround: Do not make a port with auto-QoS enabled a member of a portchannel. (CSCsi95018)

- If you configure auto-QoS on a Layer 2 port, change the port to Layer 3, and then remove auto-QoS on the port, the process will not cleanup the QoS service policies on the port due to inconsistency between when auto-QoS was applied versus when it was removed.

Similarly, if you Configure auto-QoS on a Layer 3 port, change the port to Layer 2, and then remove auto-QoS on the port, the process does not cleanly remove QoS service policies on the port.

A sequence similar to the following would lead to the problem on port g2/1

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
no auto qos voice trust
```

Workaround: Revert the port setting to the setting when auto-QoS was applied. If auto-QoS was enabled when the port was a Layer 2 port, it should be reverted to Layer 2 before auto-QoS is removed. Similarly, if the port was set to Layer 3 when auto-QoS was initially applied, it must be reverted to Layer 3 before auto-QoS is removed.

Referring to the problem sequence, first apply auto-QoS to a Layer 2 port, change it to layer 3, then revert to Layer 2 and remove auto-QoS:

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
switchport
no auto qos voice trust
```

(CSCsk95871)

- If a class-map is configured with **exceed-action drop**, re-configuring the same class-map with **exceed-action transmit** causes class-map configurations to conflict for the same class-map.

Workaround: If you plan to change a class-map action, such as **exceed-action**, you need to remove the class-map with the **no class c1** command under policy-map submenu. Then, apply the new class-map with the updated changes.

CSCsk70826)

- Applying a policy to a VLAN that has been allocated to a routed port causes the internal VLAN to be policed.

Workaround: Avoid creating a VLAN that has been allocated internally to a routed port. (CSCsh60244)

- If *exceed burst* is not explicitly configured for a dual rate policer, the **show policy-map** command displays “0” as the burst value.

Workaround: Enter the **show policy-map interface** command. (CSCsj44237)

- If *burst* is not explicitly configured for a single rate policer, the **show policy-map command** displays an incorrect burst value.

Workaround: Enter the **show policy-map interface** command. (CSCsi71036)

- When a queuing policy is attached to a trunk port configured with a per-port per-VLAN QoS policy, the port-level queuing policy is processed as part of a per-VLAN policy and is rejected on bootup. Queuing policy is supported on a physical interface in the output direction only.

Workaround: After bootup, reattach a queuing policy on a physical interface. (CSCsk87548)

- When you delete a port-channel with a per-port per-VLAN QoS policy, the switch crashes.

Workaround: Before deleting the port-channel, do the following:

1. Remove any per-port per-VLAN QoS policies, if any.
2. Remove the VLAN configuration on the port-channel with the **no vlan-range** command.

(CSCsk91916)

- The cbQosPoliceCfgTable mib object is *not* populated by the **police bps byte** command.

Workaround: None. (CSCsk45940)

- Executing **default interface** twice on a port configured with the cisco-phone macro displays the back trace.

Workaround: Remove the configuration line by line without entering the **default interface** command. (CSCsj23103)

- When you enter the **show policy-map vlan** *vlan* command, unconditional marking actions that are configured on the VLAN are not shown.

Workaround: None. However, if you enter the **show policy-map** *name*, the unconditional marking actions appear. (CSCsi94144)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

Workaround: None. (CSCsl72868)

- When you use a Catalyst 4500 series switch with Supervisor Engine 6-E with an output service policy configured on an interface, you observe output drops due to a queue full condition when you enter shut/no shut on a different interface that also has the same output service policy applied.

This issue is open in Cisco IOS Releases 12.2(40)SG, 12.2(44)SG and 12.2(46)SG.

This issue is resolved in 12.2(50)SG.

Workaround: Do not use the qos autoqos macro.

When a policy-map is shared on more than one target, it should not use any percentage based actions; police, shape, and bandwidth actions must use absolute values. This requires a different policy-map for each of the four interface speeds supported on the switch - 10M, 100M, 1G, and 10G. So, rather than having a single policy-map as enabled through percentage-based actions, you must create four distinct policy-maps. This applies to all shared policy-maps, independent of direction of service-policy.

(CSCsr12142)

- Attempting to use the nested policy-map feature on Supervisor Engine-6E can cause the switch to reboot.

Workaround: Do not use the nested policy-map feature in Cisco IOS Release 12.2(40)SG and 12.2(44)SG. (CSCsy80664)

- Output IPv6 ACLs with Ace to match on the ICMP option fail on a switch.

The following conditions may cause a RACL to malfunction:

- ACL are applied on the output direction of the interface.
- IPv6 ACL contain Ace to match on the ICMP option fields (ICMP Type or ICMP Code).

Here are two examples of such non-functioning RACL:

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20

IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

Workaround: None.

CSCtc13297

Resolved Caveats in Cisco IOS Release 12.2(40)SG

This section lists the resolved caveats in Release 12.2(40)SG:

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

Workarounds:

- Use a different copy protocol.
- Set a longer ssh timeout.

(CSCsc94317)

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

Workaround: Enter **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362)

- The switch will stop forwarding Layer 3 packets for a few seconds during either ISSU runversion or redundancy switch-over.

The traffic loss only occurs when the interfaces, which the traffic travel through, are configured with HSRP and currently in HSRP Active state.

Workaround: None. (CSCsi40980)

- If you attempts to upgrade to Cisco IOS Release 12.2(37)SG1 from the Release 12.2(31)SGA and its subsequent maintenance releases, the following harmless message is displayed upon 'issu commitversion':

```
At ACTIVE:
ISSU_PROCESS-3-SYSTEM: Failed to set Standby ISSU state to the local ISSU state.

At STANDBY:
ISSU_PROCESS-3-SYSTEM: STANDBY:System not in [Init (Commit Version)] or [Init (Commit Version)] for transitioning to [*]
```

where "*" can be "Init", "Load Version", etc.

Workaround: None. These are informative messages. (CSCsj89384)

- SNMPv3 might not work after an IOS upgrade.

Workaround: Re-apply user credentials with the **snmp-server user** command.

- A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html>

(CSCsi01470)

- If you attempt to downgrade to Cisco IOS Release 12.2(37)SG from Release 12.2(37)SG1 and if the process is started with active supervisor engine in slot-2, the downgrade fails at runversion.

Workaround: None. (CSCsj83688)

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4000 family running IOS supervisor engines:

- [Netbooting from the ROMMON, page 426](#)
- [Troubleshooting at the System Level, page 427](#)
- [Troubleshooting Modules, page 427](#)
- [Troubleshooting MIBs, page 427](#)

Netbooting from the ROMMON

Netbooting using a boot loader image is not supported. Instead, use one of the following options to boot an image:

1. Boot from a CompactFlash card by entering the following command:

```
rommon 1> boot slot0:<bootable_image>
```

2. Use ROMMON TFTP boot.

The ROMMON TFTP boot is very similar to the BOOTLDR TFTP boot, except that:

- the BOOTLDR variable should *not* be set
- the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

To boot from ROMMON, perform the following tasks while in ROMMON mode:

- a. Ensure that the Ethernet management port on the supervisor engine is physically connected to the network.
- b. Verify that bootloader environment is not set by entering the **unset bootldr** command.
- c. Set IP address of the Ethernet management port on the supervisor engine by entering the following command: **set interface fa1 ip_address <ip_mask>**

For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

```
rommon 2> set interface fa1 172.16.1.5 255.255.255.0
```

- d. Set default gateway for the Ethernet management port on the supervisor engine by entering the following command: **set ip route default** *gateway_ip_address*. The default gateway should be directly connected to the supervisor engine Ethernet management port subnet.
- e. Ping the TFTP server to ensure that there is connectivity to the server from the Ethernet management port on the supervisor engine by entering the following command: **ping** *<tftp_server_ip_address>*.
- f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://tftp_server_ip_address/<image_path_and_file_name>**

For example, to boot the image name cat4000-is-mz.160 located on the TFTP server 172.16.1.8, enter the following command:

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4000-is-mz
```

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- Ensure that you do not mix the serial and Ethernet cables plugged into the supervisor engine. The Fast Ethernet port (10/100 MGT) on the supervisor engine is inoperative in all Catalyst 4500 Cisco IOS releases. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for modules:

- When you hot insert a module into a chassis, always use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 4500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

Troubleshooting MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>). For information on the specific MIBs supported by the Catalyst 4500 series switches, refer to the Catalyst 4000 MIB Support List located at <ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html>.

Related Documentation

Although their Release Notes are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to the following home pages for additional information:

- Catalyst 4500 Series Switch Documentation Home
<http://www.cisco.com/go/cat4500/docs>
- Catalyst 4900 Series Switch Documentation Home
<http://www.cisco.com/go/cat4900/docs>
- Cisco ME 4900 Series Ethernet Switches Documentation Home
http://www.cisco.com/en/US/products/ps7009/tsd_products_support_series_home.html

Hardware Documents

Installation guides and notes including specifications and relevant safety information are available at the following URLs:

- *Catalyst 4500 Series Switches Installation Guide*
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html>
- *Catalyst 4500 E-series Switches Installation Guide*
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html>
- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html
- Installation notes for specific supervisor engines or for accessory hardware are available at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- Catalyst 4900 and 4900M hardware installation information is available at:
http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html
- Cisco ME 4900 Series Ethernet Switches installation information is available at:
http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

Software Documentation

Software release notes, configuration guides, command references, and system message guides are available at the following URLs:

- Catalyst 4500 release notes are available at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html

- Catalyst 4900 release notes are available at:
http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html
- Cisco ME4900 4900 Series Ethernet Switch release notes are available at:
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900, and Cisco ME 4900 Series Ethernet Switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- *Catalyst 4500 Series Software Command Reference*
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- *Catalyst 4500 Series Software System Message Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x
http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- Cisco IOS command references, Release 12.x
http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html
You can also use the Command Lookup Tool at:
<http://tools.cisco.com/Support/CLILookup/cltSearchAction.do>
- Cisco IOS system messages, version 12.x
http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html
You can also use the Error Message Decoder tool at:
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- For information about MIBs, refer to:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.2(54)SG
Copyright © 1999–2011, Cisco Systems, Inc. All rights reserved.

